UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
------------------------------x

UNITED STATES OF AMERICA,

v. S2 17 Cr. 548 (PAC)

JOSHUA ADAM SCHULTE,

Defendant. Trial

------------------------------x

New York, N.Y.
February 12, 2020
9:15 a.m.

Before:

HON. PAUL A. CROTTY,

District Judge
-and a jury-

APPEARANCES

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
BY: MATTHEW J. LAROCHE
SIDHARDHA KAMARAJU
DAVID W. DENTON JR.
Assistant United States Attorneys

SABRINA P. SHROFF
JAMES M. BRANDEN
Attorneys for Defendant
-and-
DAVID E. PATTON
Federal Defenders of New York, Inc.
BY: EDWARD S. ZAS
Assistant Federal Defender

Also Present: Colleen Geier
Morgan Hurst, Paralegal Specialists
Achal Formando-Peiris, Paralegal
John Lee, Litigation Support
Daniel Hartenstine
Matthew Mullery, CISOs, Department of Justice

(In open court; jury present)

THE COURT: Good morning. Happy Lincoln's birthday. Please be seated. Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

THE COURT: Mr. Leedom, I want to remind you, you're still under oath.

THE WITNESS: Yes, sir.

MR. LAROCHE: Ms. Hurst, can you please bring up Government Exhibit 1703 and go to slide 66, please.

PATRICK LEEDOM,

called as a witness by the Government,

having been previously sworn, testified as follows:

DIRECT EXAMINATION (Continued)

BY MR. LAROCHE:

Q. Mr. Leedom, yesterday you testified as to some of the changes on the DevLAN network that occurred on April 16, 2016.

A. That's correct.

Q. What were some of the changes that were made to Confluence that day?

A. On Confluence, the SSH public keys that were on the server were all deleted and replaced with a single key. And the administrative password was changed.

Q. Confluence was running on a server; is that correct?

A. That's correct.

Q. Was that an ESXi server?

A. Yes, it was.

Q. Who did that server belong to?

A. It was OSB's ESXi server.

Q. On April 16, 2016, were certain changes made to that server itself?

A. Yes, they were.

Q. Please summarize those changes.

A. On the ESXi server, the administrative password was changed.

Q. There is a sub-bullet down at the bottom that says "Schulte SSH key not removed."

A. That's correct.

Q. What is that meant to convey?

A. That the defendant's public key that was on the ESXi server was not removed. So he still had access to that server over SSH after 4/16.

Q. Prior to making these changes on April 16, did the administrators do anything to the system?

A. To the ESXi server?

Q. Let's start with Confluence. Did they do anything with Confluence?

A. The server was migrated on the 25th, but after the passwords were changed on 4/16, they made a snapshot before making the changes, but they just changed the passwords after that.

Q. What do you mean they made a snapshot before making the changes?

A. A snapshot was made before they changed any of the passwords, just in case there were any issues that arose from the passwords that they changed or the keys they deleted.

Q. You also testified that the SSH key on the ESXi server was used by the defendant on April 15 to log into that server; is that correct?

A. That's correct.

Q. Let's go to slide 84, please. We looked at this file yesterday, correct?

A. Yes, we did.

Q. You testified that this is from the auth. log of the ESXi server; is that correct?

A. That's correct.

Q. Can you show us where the administrative session was started on April 15 by the defendant?

A. The session started here. And then the session was opened here.

Q. In that number there is a -- in that circle there is a 766 number?

A. Yes, there is.

Q. What is that up?

A. That's the work ID for the defendant's session that will be logged with commands that the defendant ran in the shell log.

Q. How do you know this was the defendant's administrative session?

A. We can tell from two places, primarily. We have the IP address from the defendant's DevLAN workstation, the Ubuntu virtual machine on his workstation, and we have a fingerprint from his private key which was encrypted.

Q. What's a fingerprint from his private key?

A. It's just the unique identifier that matches the public key that was on the server, with the private key that he had on his virtual machine.

Q. Let's go to slide 76, please. You left off yesterday talking about some of the activities on April 18, 2016. Is that correct?

A. That's correct.

Q. I think you left off talking about certain administrative logins to the server itself by the defendant. Is that correct?

A. Yes, that's correct.

Q. Does this page reflect such a login?

A. Yes, it does.

Q. Starting with the top exhibit, what time did the defendant login as an administrator to the ESXi server?

A. He logged in at 11:12:08 in the morning, and the time stamp is right here.

Q. Then did he log out of the session at some point that day?

A. Yes, he did.

Q. When did he log out?

A. He logged out at 1:47.

Q. As an administrator of the ESXi server, what types of things could the defendant do on the system?

A. Primarily, manage the virtual machines, things like create snapshots, delete snapshots, list snapshots, power machines on and off; things like that.

Q. Let's go to the next slide, please. We also looked at this slide yesterday. Isn't that correct?

A. I believe so, yes.

Q. Where is this slide from?

A. This is from the ESXi server, it's from the hostd log.

Q. What does it reflect?

A. This is a login by the defendant using his DevLAN user credentials, so non-administrative credentials.

Q. A login to what?

A. To the ESXi server through vSphere.

Q. So different than the type of login on the previous slide?

A. That's correct.

Q. Let's go to the next slide, please. This slide has Government Exhibit 1209-3. Where is this exhibit from?

A. This was from the ESXi server recovered from unallocated space. It is a fragment of a log file.

Q. What does it show?

A. It shows a connection over vSphere from the defendant's workstation at about 11:12 a.m. on 4/18.

Q. Let's go to the next slide, please. This slide at the top has Government Exhibit 1209-18. Where is this log file from?

A. This is also from the ESXi server. This is from the hostd log file.

Q. What's that top slide show?

A. This is showing a login from the defendant's workstation as the root administrator user.

Q. A few slides ago we saw root login at approximately 11:12 a.m.; is that correct?

A. That's correct.

Q. Is this the same login?

A. Yes.

Q. Were there two logins or one login at 11:12 a.m.?

A. There were two logins; one was shortly after the other.

Q. Is this the second login?

A. Yeah, that's correct.

Q. How do you know this is a different login?

A. We can match up the login and log out, like time stamps for the sessions, and determine that there were two separate logins.

Q. At what time did he log out of this session?

A. Is it just me or it's flashing here?

Q. Did you lose the screen?

A. Yes. It's flashing in and out. Okay. Maybe it's just me.

Now I have nothing. Oh.

THE COURT: Do you have a hard copy for him?

MR. LAROCHE: Yes, your Honor.

A. Let me see if I can move it. Now it's gone completely.

THE COURT: Does the jury have the same problem?

A JUROR: No.

THE COURT: You can see?

A JUROR: Yes.

Q. Mr. Leedom, we're on slide 79.

A. Give me just a second. I can draw but there's no -- just a second.

THE DEPUTY CLERK: Mr. Leedom, anything?

THE WITNESS: No.

A. I've got slide 79.

Q. We'll go through the hard copy, that's fine. I think the jurors still have it.

A. Okay. I'll try and explain geographically what I'm talking about.

Q. So, we're on slide 79 and we see another login at 11:12 a.m. as root. Is that correct?

A. That's correct.

Q. You just testified that there were two logins at 11:12 a.m.; is that correct?

A. Yes, that's correct.

Q. At what time approximately did the defendant log out of this session?

A. About 11:43 a.m.

Q. Let's go to the next slide, please. Now we're on slide 80. This shows Exhibit 1209-3 again.

Where is this exhibit from?

A. This is from the ESXi server recovered from unallocated space.

Q. Again, what is this showing?

A. This is showing a connection from the defendant's workstation to the ESXi server over vSphere and we can see --

Q. For what login does this show?

A. I'm sorry. Could you repeat the the question?

Q. Sure. What login does this show?

A. This shows the login at 11:12 a.m.

Q. This is a server-side log; is that correct?

A. That's correct.

Q. On the previous slide, that was also a server-side log; is that correct?

A. That's correct.

Q. Let's go to slide 81. This is showing Government Exhibit 1202-3. Where is this exhibit from?

A. This is from the defendant's DevLAN workstation in his downloads folder.

Q. What does this exhibit show?

A. This shows that a web page was downloaded of a specific page on Confluence at -- on April 18, at 2:01 p.m.

Q. What page was downloaded by the defendant?

A. The page name was the OSB's ESXi server page.

Q. Let's go to the next slide, please. Is this the exhibit that the defendant downloaded, this page?

A. Yes, this is part of it.

Q. Where is this from?

A. This is, this is a picture of, if you open that file, this is what you get.

Q. If we can zoom in on the infrastructure VMs at the bottom. As of -- before April 16, 2016, what was the root password for the ESXi server?

A. Before April 16, the root password was My Sweet Summer.

Q. Did that change?

A. Yes, it did.

Q. When did it change?

A. It changed on April 16, when they reset the passwords.

Q. Did it remain My Sweet Summer?

A. No, it did not.

Q. Let's go to the next slide, please. This is showing Government Exhibits 1209-21 and 22. Where are these exhibits from?

A. This is from the ESXi server.

Q. What is this showing?

A. This is showing a login as the root account to the ESXi server through vSphere.

Q. Whose login is it showing?

A. It is the root login, so the administrator login.

Q. By who?

A. From the defendant's workstation.

Q. How do you know that?

A. We have his IP address, if you look in the top-right-hand corner.

Q. At what time did he log in?

A. About 7:17 p.m.

Q. At what time did he log out?

A. About 7:47 p.m.

Q. If we go to the next slide, please. We've seen this slide come up several times; is that correct?

A. That's correct.

Q. We just talked about several administrative logins to the server on the last few slides, correct?

A. That's correct.

Q. Does this slide reflect a different kind of administrative login?

A. Yes. This slide only shows logins with the password for the server itself. Or the SSH key to the actual server itself.

Q. This a session that was given an ID 766; is that right?

A. That's correct.

Q. Did you see any evidence of the defendant using this administrative session on April 18, 2016?

A. Yes, I did.

Q. Let's go to the next slide and take a look at that. This slide has Government Exhibit 1203-43. There is some highlighted text there.

A. Yes.

Q. First, where is this exhibit from?

A. This is from the defendant's DevLAN workstation in his Ubuntu virtual machine recovered from unallocated space.

Q. Let's zoom in on the highlighted section, please. What do these lines show?

A. These lines show commands that were entered on the ESXi server by the defendant, and we know that from this session ID, the 766 number, on April 18, which we know from the time stamp on the left.

Q. Do these reflect commands that were run using the ESXi server administrative session?

A. Yes, over SSH.

Q. What are some of the reasons these commands were recorded in the unallocated space of the defendant's computer?

A. Since we have a record of the actual text output that was output to the defendant's screen, that we were able to recover, at some point, he viewed the contents of the shell.log file and we have those here.

Q. If we can zoom out again. At approximately what time did the defendant run these commands?

A. About 6:08 p.m.

Q. So let's go to the next slide. I want to walk through how we know it was that defendant's administrative session that was being used. So let's start with the first point.

What is that point meant to convey?

A. On April 15, there was a login to the ESXi server which we've seen multiple times from the auth. log file, which used his encrypted private key. The password to that key was KingJosh3000.

Q. The second bullet says "Work ID assigned to that session was 11130766."

What's the significance of a work ID for that session?

A. So, work IDs are assigned to a session when the session is open. I'll cover a couple in the next points. They're unique IDs, so two users would never have the same work ID. They don't change while the session is active, so for the entire time the session is active the work ID will remain the same. And they're saved in that shell.log file, of which a piece we were just currently viewing, to attribute commands to a particular session. So you can know who was running what commands on the server.

Q. You've mentioned shell.log several times. What is shell.log?

A. Shell.log is a log file on ESXi that keeps command history for commands that were run on the server.

Q. Is that type of log file important to auditing user activity?

A. Oh, it's extremely important.

Q. Why?

A. It's one of the few places where you can actually see what commands a certain user was running on a system.

Q. And the last point says "The work ID session ending in 766 never ended."

A. That's correct.

Q. How do you know that?

A. We never have a log in the auth. log file that says the session was closed and that the session disconnected.

Q. So let's go to the next slide, please. We're now in slide 87 which is Government Exhibit 1209-8. Where is this exhibit from?

A. This exhibit is from the ESXi server in a recovered file location for the shell.log file called file slack.

Q. If we can zoom in on that exhibit, please. You said it's file slack?

A. That's correct.

Q. What's file slack?

A. So, file slack in most modern file systems, when the computer allocates space for a file, the -- there is a certain minimum amount of space that has to be allocated for that file to be stored. You'll hear them referred to as blocks or clusters. When a file is modified, the parts of the file kind of change, they get larger and smaller inside that cluster. And when things are deleted from that file, you can go to the cluster where that file was stored, and look after the file is supposed to end, and find additional data in that cluster.

A good analogy is if you have like a shoebox with shoes in it. The shoes are like the resident part of the file that you would see if you opened it on your computer, and the file slack would be the space that's the empty space in the box around the shoes.

Q. So what did each of the lines on this exhibit show?

A. Each of these lines is a different command that was entered on the ESXi server. And all of these lines belong to the defendant.

Q. How do you know that?

A. All of these lines are tagged with the work ID from the session that the defendant initiated.

Q. This isn't the actual shell.log, is it?

A. It's not the shell.log that appears on the server to this day.

Q. Is there a shell.log that appears on the server today?

A. Yes, there is.

Q. Does that shell.log reflect these entries?

A. No, these entries are not in that file.

Q. Do you have an opinion as to why that is the case?

A. Yes, I do. If you can look at the, there is, I don't know exactly what you guys have blown up. But there is a bit of white space towards the top corner. The last command before that white space is VIshell.log. Now, VI command on most Linux systems is a, it is a command for a text editor. So this would allow you to edit the contents of a file. And it's very telling, seeing it especially as the last entry in this case and not seeing these entries in the original file. It is indicative that they were deleted.

Q. Is it standard practice to delete command history from shell.log?

A. No, it's not.

Q. Why not?

A. It's, like I mentioned before, it's one of the only ways you can attribute commands that a certain user was running on the server. And you would never delete those commands.

Q. Let's go to the next slide, please. Let's just zoom in on this. So, showing you a portion of the last exhibit, one of the command lines.

A. That's correct.

Q. When was this command run?

A. This command was run at 6:37 p.m. on April 18.

Q. By whom was it run?

A. By the defendant.

Q. Did you see evidence of this command on the defendant's DevLAN computer?

A. Yes, we did.

Q. Let's go to the next slide and take a look. So the top of this slide shows that same command from Government Exhibit 1209-8. Is that correct?

A. That's correct.

Q. At the bottom there is Government Exhibit 1203-44. You see that?

A. Yes, I do.

Q. Where is that exhibit from?

A. The bottom exhibit is from the defendant's DevLAN workstation from his Ubuntu virtual machine recovered from unallocated space.

Q. Just focusing on that exhibit. How do you know this is a command run on the OSB ESXi server?

A. If you see the front of that bottom exhibit, it says root@OSB. That's how we know it was the OSB server.

Q. What command was run?

A. This is a file listing command. It's similar to the ones we've seen before. It is essentially just telling the computer to show me all the files in this specific folder, the folder is /var/run/log.

Q. Let's go to the next slide. On slide 90. You see at the top of the page that command line?

A. Yes, I do.

Q. What's the rest of the exhibit showing here?

A. This is showing part of the output from that command.

Q. Let's go to the next slide, slide 91. Again at the top we have Government Exhibit 1209-8, that command line. What's the bottom exhibit showing?

A. This is the completion, so the last couple rows of that LS command.

Q. At what time approximately was that LS command run?

A. The command was run in about 6:37 p.m.

Q. How do you know that?

A. If you look at the third line up from the bottom, you can see the VPXA.log file in the file listing, and just to the left of it there is a time stamp for the last time that file was modified. And as I testified earlier, some of the log files inside of the log folder on the ESXi server are updated every second, if not faster than that, which updated this modify time. So it gives us a fairly accurate time stamp as to when the LS command was run.

Q. So, let's focus on the top exhibit for a moment. You testified earlier that that was in UTC time; is that correct?

A. That's correct.

Q. How do you know that?

A. When the time stamp's displayed this way in kind of an extended format, the Z is appended to show that it's in UTC time.

Q. Then just look at the bottom exhibit for a second. There is the 22:37 three lines from the bottom. Do you see that?

A. Yes.

Q. There's no Z next to that.

A. No, it's not.

Q. What time zone is that?

A. It's in UTC time.

Q. How do you know that?

A. So the LS command is meant to display things in a convenient and easily readable way. With the flag that's been provided here, it just displays like the simple time and it doesn't give, like, the time zone information. But all the log files on the ESXi server were -- the time stamps are going to be displayed in UTC.

Q. Let's look at one more example of some of the commands that were run on April 18. We can go to the next slide, please. Again, is this another command line from that shell file slack?

A. Yes, it is.

Q. Is this the next command that was run after the command we just saw?

A. Yes, it is.

Q. If we can just focus on that bottom command. It's LS-AL//VAR.

A. That's correct.

Q. What are the two back slashes there?

A. The two -- they're actually forward slashes, but the two forward slashes, it could just be a typo. You would, to list the files at slash var, you just have to give one slash.

Q. So you wouldn't need to do two forward slashes to run the command; is that correct?

A. Not to my knowledge, no.

Q. Did you see evidence of this command being run on the DevLAN land's computer?

A. Yes, I did.

Q. Let's take a look at that. Go to the next slide, slide 93. What is the bottom exhibit showing?

A. So the bottom exhibit is showing the end of the command that we just reviewed two slides ago, and the command immediately following that.

Q. At approximately what time was that second command run?

A. I don't believe the time stamp's on this slide, but it would be some time after 6:37 p.m., the output of this list command should list the exact time.

Q. Do you see the bottom slide also has the two forward slashes?

A. Yes, it does.

Q. Is that the same command that appears in the file slack?

A. Yes, it is.

Q. Let's go to the next slide. This slide is titled "Recap, April 18, 2016." If you could just walk us through, starting with the top bullet, some of the things that happened on DevLAN that day.

A. Sure. So, at the beginning of April 18, at about 11:12:08 and 11:12:18 in the morning, the defendant logged in as root to the ESXi server.

At 11:43 a.m., the defendant logs out as root to one of those sessions.

Around 12:59 p.m. the defendant e-mails Anthony stating that "It seems like overnight all my permissions on the servers themselves revoked."

At 1:47 p.m., the defendant logs out as root to the other session on the ESXi server.

At 2:01 p.m., the defendant downloads the old ESXi server page from Confluence.

At 7:17 p.m., the defendant logs in as root to the ESXi server again.

Between 6 and 7:44 p.m., the defendant used his administrative session, that's the SSH session from the shell log that we've been viewing for the last few slides, to view various log files on the server.

Q. Let's go to the next slide. I'd like to talk about some of the activities on April 20, 2016. Go to slide 96. This slide is titled "Overview."

Generally, what is this slide meant to convey?

A. This is just a simple overview of the activities that occurred on April 20.

Q. Let's start with the first bullet. What does the first bullet reflect?

A. So, at 5:35 p.m., the defendant used administrative privileges on the ESXi server to revert the Confluence virtual machine to a snapshot that was created on April 16, 2016.

Q. In its reverted state, what accesses would the defendant have had to Confluence?

A. All of the administrative accesses, since this snapshot was taken before the passwords were changed.

Q. Why is that?

A. All the passwords were still in place on the server, because they hadn't been changed or deleted yet.

Q. In Confluence's reverted state, would the defendant have had access to the mount points for the Altabackups?

A. Yes.

Q. How would he have gotten to the mount points at that point?

A. He could have simply navigated to the /mount/Altabackup folder on the server.

Q. The second bullet, sorry. What does the second bullet reflect?

A. So, the Confluence virtual machine remained in the reverted state for a little over an hour until approximately 6:51 p.m.

Q. Would that have been enough time for the defendant to copy a backup of Confluence?

A. Yes, it would have.

Q. What about a backup copy of Stash?

A. Yes, it would have.

Q. Let's go to the third bullet. What's that meant to convey?

A. At about 5:43 p.m., the March 3, 2016 Confluence backup file was accessed in the Altabackups folder on the NetApp server.

Q. How do you know that that file was accessed around that time?

A. The access time for the file was updated on the server.

Q. What computer actions would update the accessed folder?

A. File reads and copies in this case.

Q. Do you have an opinion as to what computer action caused the date accessed to update at that time?

A. Yes, I do.

Q. What is your opinion?

A. It was a file copy.

Q. By whom?

A. By the defendant.

Q. What are some of the reasons for that opinion?

A. The defendant was in a location that had access to those backups. And then shortly after, we see the file accessed. We see all the log files related to things that would tell us how those accesses happened from that server being deleted, as well as all of the -- well, not "all," but many log files from the ESXi server also being deleted.

Q. So let's talk about that for a second. What is the fourth bullet meant to convey?

A. Between about 5:50 and 6:58, so this encompasses the duration of that reversion and shortly after, the defendant deleted logs of his activities.

Q. Let's walk through April 20. Let's go to the next slide, please. This slide has Government Exhibit 1067 which is an e-mail sent on April 20, 2016, at 12:06 p.m. From Mr. Weber to EDG staff.

Can you please read the text of that e-mail.

A. Yes, I can. "All, on Monday, April 25, at 6 a.m., ISB will be migrating the Bamboo and Confluence servers to new hardware and will need to power them down for a limited amount of time. To ensure no work is lost, please log out of Confluence and Bamboo when you depart on Friday. If this maintenance window will cause any issues for you, feel free to contact me." Signed Jeremy Weber.

Q. Let's go to the next slide, slide 98. This slide has Government Exhibit 1069, an e-mail sent on April 20, 2016, at 3:58 p.m.

Can you please read the first two sentences of this e-mail.

A. Yes, I can. "On Monday, 25 April, from 0600 to 1000 hours, the Atlassian suite (in particular the Bamboo and Confluence servers) will be unavailable due to maintenance. SED/ISB will be transferring the data to new servers/hardware to bring the DevLAN Atlassian suite under SED/ISB configuration management in accordance with EDG best practices."

Q. Now, what impact would the transfer of Confluence and Bamboo off the ESXi server that OSB was running have on somebody's ability to use Confluence and Bamboo on that server?

A. Well, they wouldn't be on that server anymore. They were migrated to a different server.

Q. If someone had administrative privileges to OSB's ESXi server, and Confluence and Bamboo were no longer there, could they do anything to those virtual machines anymore?

A. No, they would not be able to.

Q. Let's go to the next slide, please. So this slide contains Government Exhibit 1202-13.

A. Yes.

Q. Where is this exhibit from?

A. This is from the defendant's DevLAN workstation from a log file that logged chat logs from a protocol chat application called IRC.

Q. What is IRC?

A. It stands for Internet Relay Chat. It's just a text based chat application where you can talk to users between different computers.

Q. Where were these chats found?

A. These chats were found on the defendant's workstation in a log file that was logging records of the chat messages sent on various channels.

Q. Let's look at the top portion of this slide, please.

A. Yes.

Q. What does this show?

A. This shows some administrative type commands being run for the IRC server. The first command AOP, and AOP is like an administrative operator on IRC, so it's just a user that has permissions to modify the channel, set like message of the day, things like that. The list command shows the list of all of the people who have those permissions. And this is just the output from that, showing those users.

After the list command, there's an attempt to remove the user Jeremy Weber from the OSB channel operator's list. And then an error from the server saying that the syntax is wrong. Essentially, the word "remove" is not the correct way to delete someone from that list.

Q. Let's go to the bottom part of this slide, please.

A. So at the first part of this bottom slide, and we can see it from the end of the top slide, where it gives the correct version of the command. Essentially instead of the word "remove," you need to use the word "DEL" for delete instead. We have a operator for channel OSB delete Weber, so it will delete this user from OSB as an administrator, and then the server says "permission denied."

After that -- "permission denied" just means the user who tried to do the delete didn't have permission to make the deletion. After that, we see the defendant set permissions to himself, give him all the permissions required to perform this deletion action, and you can see that it's successful. You are now an IRC operator. Global from operator server Schuljo is now an IRC operator. Then we see the user Jeremy Weber is deleted from four or five different channels.

Q. At what time approximately did these actions occur on April 20?

A. They were about 4:06 p.m.

Q. Let's go to the next slide, please. Is this just a zoom in on the previous slide?

A. Yes, it is.

Q. Let's go to the next slide. This is Government Exhibit 1202-12. Where is this exhibit from?

A. This is from the same place as the last exhibit, it is a log from IRC from the defendant's DevLAN workstation.

Q. What does this show?

A. This is showing another channel that the defendant deleted Jeremy Weber from. The Bamboo channel, specifically, and then listing of the access to that channel and a list of the users who have admin access.

Q. Okay. Let's go to the next slide, please. This is titled "April 20, 2016, Recap Before 5 p.m."

Does this just reflect the e-mails and the chat deletions we just viewed?

A. Yes, it does.

Q. Let's go to the next slide. Still on April 20, 2016, and we're talking about activities between 5 and 5:30 p.m., is that right?

A. That's correct.

Q. What does this slide summarize?

A. At about 5:18 p.m., Rufus's key was accessed. At 5:19, defendant connected a Sandisk USB device to his Ubuntu virtual machine. And at 5:29 p.m. the defendant created a snapshot titled bkup for the Confluence virtual machine.

Q. So let's walk through each of those. We go to the next slide, slide 104. This is Government Exhibit 1207-1. Where is this exhibit from?

A. This is a file on the NetApp server in the home folder, specifically the defendant's home folder.

Q. What is this file showing?

A. This is a private key file for like an SSH public private key pair for a different user on the DevLAN network called Rufus.

Q. You see there is an accessed down near the bottom?

A. Yes, I do.

Q. What does that reflect?

A. This reflects the last time that this file was accessed.

Q. What types of computer actions will update the accessed?

A. Quite a few. You could, if you right clicked on the file to view the properties, if you used this file with an application, things like that would update the accessed time. If you copied the file to somewhere else.

Q. Let's go to the next slide.

MS. SHROFF: Your Honor, may I just have one minute with Mr. Laroche?

THE COURT: Yes, if Mr. Laroche wants to talk to you.

MR. LAROCHE: Sure, your Honor.

(Counsel conferring)

MS. SHROFF: Thank you, your Honor.

MR. LAROCHE: We're all set, your Honor.

THE COURT: We're trying to make some technical corrections here on the fly.

MR. LAROCHE: Sure. Understood.

A. Are we on slide 105?

Q. Yes, we are thank you. This slide has Government Exhibit 1203-54. Do you see that?

A. Yes, I do.

Q. Where is this exhibit from?

A. This exhibit is from the defendant's DevLAN workstation from a log file that comes from that Ubuntu virtual machine that we've been discussing on his workstation.

MR. LAROCHE: If we can just zoom in on the log file, Ms. Hurst.

Q. What is this log file showing?

A. So this, the VMware log file will show when external devices are connected to virtual machines. In this case, this is showing that some USB devices were passed through from the host computer to the virtual machine on that computer.

Q. I think the title of this slide has a Sandisk USB device; is that correct?

A. That's correct.

Q. Can you point out that Sandisk USB device in this exhibit?

A. Yes. It's right in the middle. You see USB found device, name, Sandisk Extreme. Then some serial number information.

Q. You see next to found device there is a T8R2?

A. Yes, right above it.

Q. What does that mean?

A. That's a separate device. This log is showing three devices in total. The first device, T8R2, to my knowledge is a Tableau, Tableau is a company that makes forensic hardware devices. It is a write blocker.

So I'll explain a write blocker quickly. You use a write blocker when you want to prevent a computer from making changes to external media. So, if you plug like a USB drive into the write blocker and you try to write changes to the USB drive, it won't let you do that. It keeps it forensically pure.

The third entry here you see virtual Bluetooth adapter. That is just a VMware stock Bluetooth adapter. It's not really of consequence in this log for what we're looking at.

Q. What significance, if any, is there to a write blocker being on the USB device?

A. If the write blocker is connected to the USB, it means data couldn't be written to the USB device. Only read from it.

Q. Let's go to the next slide. This is showing Government Exhibit 1202-16. Where is this exhibit from?

A. This exhibit comes from the defendant's DevLAN workstation. This is one of those VI client logs, so this is a log related to activities taken in that vSphere application.

Q. Where are VI client logs stored?

A. They're stored on the client. So in this case the DevLAN -- the defendant's DevLAN workstation.

Q. Are they also stored on the server?

A. VI client logs are not stored on the server.

Q. What does this log show?

A. This log shows, so the way that the vSphere application works, if you click a button on the UI, it makes a request to the server and the server has to send back a response. So in this case, we're looking at a list of snapshots, so if you clicked the button on vSphere to show available snapshots or manage snapshots for the Confluence virtual machine, this is the data that server is sending back. So, when that button was clicked, the server sent back that there were two snapshots available for that virtual machine at 5:29 p.m. on April 20.

Q. Who ran these commands?

A. The defendant.

Q. How do you know that?

A. This is a VI client log from the defendant's workstation, from his vSphere. So they wouldn't be from, like, another machine or something like that.

Q. How many available snapshots were there at 5:29 p.m.?

A. Only two snapshots.

Q. You see where it says "virtual machine snapshot: 57"?

A. Yes, it's in that bottom third of the image.

Q. What does the 57 refer to?

A. 57 is the machine identifier for the Confluence virtual machine on the ESXi server.

Q. Let's go to the next slide. This has Government Exhibit 1202-17. Where is this exhibit from?

A. This exhibit comes from a VI client log file on the defendant's DevLAN workstation.

Q. If we can just zoom in on the text there, please. What is this log file showing?

A. So this is showing when a snapshot is created on the virtual machine through the vSphere application.

Q. At what time was a snapshot created?

A. At 5:29 p.m.

Q. On what day?

A. April 20, 2016.

Q. What was the title of that snapshot?

A. The name of the snapshot was bkup. If you look at the fourth line of the log, you can see name, bkup, name just in the element.

Q. Who names the snapshot?

A. The user that makes the snapshot names the snapshot.

Q. Let's go to the next slide, please. This is Government Exhibit 1203-25. Where is this exhibit from?

A. This exhibit is from the defendant's DevLAN workstation in the Ubuntu virtual machine recovered from unallocated space.

Q. If we could zoom in on the text, please. What is it showing?

A. So since we have the activity that was displayed on the screen, when from the defendant's administrative SSH session on the ESXi server, at some point, he viewed the contents of one of the server logs on the server that was eventually deleted, and we're just seeing the contents of that server log file here. Specifically, if you look at the top line, you can see "initiated lazy snapshot, bkup:3." This is just the server-side confirmation that a snapshot was being created.

Q. You said it reflects a server-side log. Is that correct?

A. That's correct.

Q. You also referenced that those logs were deleted?

A. Yes.

Q. Who deleted those logs?

A. The defendant deleted the logs.

Q. Let's go to the next slide, please. This is Government Exhibit 1209-7. Where is this exhibit from?

A. This is from the ESXi server itself, recovered from unallocated space.

Q. What is it showing?

A. This is showing another, just another server-side confirmation that a snapshot was requested and created by the root user. If you see the second line about halfway in, you see user equals root. That just says the root user requested the snapshot to be created. Then it shows some of the state transitions that the machine has to go through to create the snapshot. It also shows that this is the Confluence virtual machine. And then at the bottom, I don't know if -- at the bottom in part two, it shows that the snapshot was completed.

Q. What permissions did the defendant use to create the snapshot titled bkup?

A. Administrative permissions.

Q. How do you know that?

A. If you see, look at the second line about halfway in, you can see user equals root, and that's how we know it was the root user who made these actions.

Q. You stated that this exhibit comes from the unallocated space of the ESXi server. Is that correct?

A. That's correct.

Q. Do those logs come from any particular type of file on the ESXi server?

A. Yes. We can see about a third of the way in on the first line, it says "info hostd." The log file this would have been in is log file called hostd.log.

Q. Does the hostd log file exist on the current state of the ESXi server?

A. No, it does not.

Q. Why not?

A. It was deleted by the defendant.

Q. Let's go to the next slide, please. This slide just has a recap of 5 p.m. to 5:30 p.m., is that correct?

A. We're almost there. Now I just can't draw.

Yes, it does.

Q. This is slide 110 that you're on; is that correct?

A. That's correct, yes.

Q. Let's go to the next slide, which is titled "Overview of 5:30 p.m. to 6:55 p.m."

What are some of the things that happened during that time frame?

A. During that time frame, the defendant, at 5:35 p.m., reverted the Confluence VM to that 4-16-2016 snapshot.

Between 5:35, after that snapshot was reverted, and about 6:51 p.m., Confluence remained reverted in that reverted state for a little over an hour.

At 6:51 p.m., the defendant reverted back to this bkup snapshot that we saw he just created.

At 6:51 p.m., we see the defendant listing all of the available snapshots for the Confluence virtual machine.

And then at 6:55 p.m., the defendant deletes that bkup snapshot by erasing all the activity on the server for that last hour.

Q. So let's walk through each of those steps. We can go to slide 112. It has Exhibit 1202-18. Is this another VI client log?

A. Yes, it is.

Q. What does this show?

A. This is showing the snapshot reversion to the first snapshot, the BK 4-16-2016 snapshot.

MR. LAROCHE: If we can just zoom in, Ms. Hurst, on the top three lines, please.

Q. How do you know that from the top three lines?

A. At the end here, this is the name of the snapshot. And then this "show warn" here, the way the -- this server client interact works with vSphere, this likely popped up some kind of visual warning and the message for that warning was "Confirm: Current state of the virtual machine will be lost unless it has been saved in a snapshot. Revert to snapshot BK 4-16-2016."

Q. If we can zoom out, please. At what time did the defendant revert to the snapshot BK 4-16-2016?

A. 5:35 p.m. on April 20.

Q. Let's go to the next slide, please. This is 1202-19. Is this another closer version of the same slide from before?

A. No. This is the reversion about an hour later to the bkup snapshot.

Q. So it is a different reversion?

A. Yes, it is.

Q. What reversion does this show?

A. This is showing the reversion to that bkup snapshot, otherwise known as snapshot 3 at the end of that hour period.

Q. You see at the top it says "Current state of the virtual machine will be lost unless it has been saved in a snapshot."

A. Yes, I do.

Q. What's that mean?

A. The way running a virtual machine works, if you ever go from one saved state to another saved state, you lose all of the current activity that has been occurring on the server since the last snapshot was taken.

So, at a high level what happened was the defendant created a snapshot like as things are right now. And then so that saves the state of how things were at that point. That's the bkup snapshot. And then reverted to an earlier time, back on 4/16 when accesses were available, and then stayed on that chain for a while, for a little over an hour. And then reverted everything back to where they were at the beginning, when the bkup snapshot was made. And then deleted that snapshot to show there was like no evidence of that snapshot being made.

Q. So, what impact would the reversion back to bkup have on evidence of things that happened during the reversion?

A. It would erase all evidence of everything that happened during the reversion.

(Continued on next page)

BY MR. LAROCHE:

Q. And why is that?

A. Since there's no -- and it tells you. It says unless it has been saved in a snapshot. If you wanted to save activity of what happened there, you would have to take an additional snapshot to save that period of activity. But since that didn't happen, there's -- there's -- all that activity's lost.

MR. LAROCHE: Let's go to the next slide, please.

Q. This is showing Government Exhibit 1202-20. Is this another VI client log from the defendant's computer?

A. Yes, it is.

Q. What does this log show?

A. So, similar to before when we saw a listing of snapshots, this is when the defendant clicked the button on vSphere that said, like, manage snapshots, and this is the server response just saying: Hey. I've got three snapshots available. Which one do you want to work with?

Q. At this point, at 6:51 p.m. on April 20, how many snapshots were available?

A. There's three snapshots.

Q. Which snapshot was the snapshot titled "BKUP"?

A. It's snapshot 3, which we can see right here.

MR. LAROCHE: Let's go to the next slide, please.

Q. This has Government Exhibit 1202-21. Is this another VI client log?

A. That's correct.

MR. LAROCHE: Let's zoom in on this, please.

Q. What is this log showing?

A. This is another warning message from vSphere that says: "Confirm delete. Are you sure you want to delete this snapshot?" And then this snapshot is in reference to snapshot 3.

And then at the bottom end of this, we see that the snapshot deletion was completed at 6:55 p.m.

Q. And snapshot 3 was the BKUP snapshot, is that correct?

A. That's correct.

Q. And does this reflect that it was successfully deleted?

A. Yes, it does.

MR. LAROCHE: OK. Let's go to the next slide, please.

Q. And we looked at this slide yesterday, is that correct?

A. Yes, we did.

Q. And this is from Confluence, is that right?

A. Yes. This is a configuration file for the Confluence virtual machine.

Q. I think you stated yesterday this shows the available snapshots. Is that right?

A. Yes, it does.

Q. Where is the snapshot 3?

A. It is not on this list.

Q. Why not?

A. It was deleted as a snapshot on the system so it's not tracked in the available snapshot list.

MR. LAROCHE: Let's go to the next slide, please.

Q. And this slide just has a recap of the things that you testified about, about some of the things that happened during that time frame, is that correct?

A. That's correct.

MR. LAROCHE: Let's go to the next slide.

Q. This is titled "April 20, 2016, activities between 5:29 p.m. and 7:00 p.m." Now, we just talked about some activities during that time frame, is that correct?

A. Yes, we did.

Q. Were you able to identify other activities that occurred during that time frame?

A. Yes, I was.

Q. And how were you able to do that?

A. Primarily through the unallocated space from the Ubuntu virt. machine on the defendant's DevLAN workstation that recorded history of his SSH session to the ESXi server on April 20.

Q. Let's look at the first bullet here, at 5:29 p.m. What is that meant to convey?

A. This is saying the defendant's -- the defendant used that SSH session to run the list command for log files, and the size total of those files was about 28,030.

Q. Let's look at that list command.

MR. LAROCHE: Let's go to the next slide, please.

Q. This is showing Government Exhibit 1203-1. And where is this exhibit from?

A. This is from the unallocated space in the Ubuntu virtual machine on the defendant's DevLAN workstation.

Q. And what is it showing?

A. This is showing a list command with the flags ALTR.

Q. And what privileges were used to run this list command?

A. This was the root administrative session on the server through the SSH connection.

Q. How do you know that?

A. We know that from the prompt; we see root@OSB.

Q. And where is the defendant listing log files?

A. The folder here is quite long. I'll circle it.

This is the main log file location for the ESXi server. This "VMFS/volume/" big number "/log" is the path to that location.

Q. And you said main log file location, is that right?

A. Correct.

Q. What do you mean by that?

A. So, by main log files, I just mean the ESXi server logs.

The server also keeps log files for individual virtual machines that it operates, but those are going to be stored specific to those virtual machines.

MR. LAROCHE: Let's go to the next slide please.

Q. What is this slide showing?

A. This is showing a, just a continuation of the output from that LS command.

MR. LAROCHE: Let's go to the next slide, please.

Q. What is this showing?

A. This is showing the end, so at the very bottom, the completion of that LS command.

Q. And approximately when was that list command run?

A. That list command was run at 5:29 p.m.

Q. How do you know that?

A. We can see that from the time stamps of the modified times of these files. And like I said earlier, these files get updated very, very frequently. And you can see that all of them are updating -- actually, they're all updating pretty frequently.

Q. Do you see at the bottom the bottom row has shell.log?

A. Yes, I do.

Q. What significance do you take from the 5:29 p.m. attached to the shell.log?

A. That means that the shell.log file was updated at 5:29 p.m. And we know the shell.log file stores command history information for commands that were entered into the server. So this says that, like, the current, most, like, recent entry on that file will be from a command run at 5:29 p.m.

Q. And what was the total log files that came from this list command?

A. It was 28,030. It's the number -- that number's not like kilobytes or megabytes. It's the count, number of individual 512-byte blocks that the files inside it occupy. It's just a way that LS kind of gives you a rough file-size estimate of what's in the folder.

MR. LAROCHE: If we can just go back one slide -- or two slides, please.

Q. What was the actual command that was run, the LS command? What was it?

A. Yeah. So, it's LS, and then the flags, which I described, I believe, the first two earlier. LS-ALTR.

MR. LAROCHE: Sorry. We'll come back to that in a second.

Q. LS/ALTR, is that correct?

A. That's correct.

MR. LAROCHE: Let's go to slide 123.

Q. Exhibit 1203-2, where is this from?

A. This is from unallocated space in the Ubuntu virtual machine on the defendant's DevLAN workstation.

Q. What is this showing?

A. This is showing an entry for the shell.log file -- well, an entry from the shell.log file from April 20.

Q. And do you see the 11130766?

A. Yes, I do.

Q. What is that number?

A. This is the identifier that we've been referring to. That's the defendant's SSH session to the ESXi server that was initiated on April 15.

Q. At what time does this log file reflect activity being run?

A. This time is 5:29 p.m. on April 20.

Q. And what command does it reflect being run at 5:29 p.m.?

A. The LS-ALTR command.

Q. What is the significance of this exhibit to your opinions?

A. This shows us that the defendant was on the ESXi server in that same session that he created on 4/15 on April 20. And we know from the time stamp on the previous slide that this is the command that was entered that updated the modified time of that shell.log file.

MR. LAROCHE: Let's go to the next slide.

Q. And this is the auth.log that you've talked about several times, is that right?

A. Yes, it is.

Q. And again, can you circle the 766 session that you just referred to?

A. Yes, I can.

Q. Can you circle the defendant's IP address connected to that session?

A. Yes, I can.

MR. LAROCHE: OK. Let's go to the next slide.

And let's go to the next one, 125.

Q. This is also titled "activities between 5:29 p.m. and 7:00 p.m." And you see at the bottom there there's a bolded bullet point. Do you see that?

A. Yes, I do.

Q. What is that meant to convey?

A. This is showing the time that that Confluence backup file, both the database file and the home directory, were accessed in Altabackups.

MR. LAROCHE: Before we go to that, let's go to the next slide.

Q. This is titled "The defendant's reversion to the April 16, 2016, snapshot." What effect would that have on his accesses to the system?

A. It essentially resets the access to the Confluence virtual machine to everything it was before they changed the passwords on 4/16.

Q. And so what are some of those privileges that would have been reset?

A. All of the SSH keys were still available to be logged in with; the original password to the server. The Altabackup mount point was still there, and it stayed throughout the whole time. It never got removed. It was still there as of April 25 as well.

And, yeah, just essentially the credentials and everything that you would need to access it is what you would have needed on April 16 or before that.

Q. And without administrative access to the Confluence virtual machine, could a regular user access the mount point to the backups?

A. No, they could not.

Q. Why not?

A. Because the mount points can only be accessed by an administrative user in a, like, terminal or shell session with the server. Someone browsing to the Confluence web page to view an article wouldn't be able to access those files.

MR. LAROCHE: Let's go to the next exhibit, please.

Q. Showing you portions of 1207-27 and 1207-30, and I want to focus on the top exhibit.

MR. LAROCHE: If we could zoom in on that.

Q. Looking at the March 3, 2016, SQL file for Confluence, what is the date-accessed time?

A. The date-accessed time is April 20, 2016, at 5:42 p.m.

MR. LAROCHE: If we could go to the bottom exhibit.

Q. Same question for the TGZ file; at what time was it accessed?

A. The March 3 TGZ file was accessed at 4/20, 2016, at 5:43 p.m.

Q. And at what time did the defendant revert Confluence to the

4/16, 2017, snapshot?

A. About seven or so minutes prior, at 5:35 p.m.

Q. Now, as part of your review in this case, have you reviewed the Altabackups folder for Confluence?

A. Yes, I have.

Q. Other than the March 3, 2016, backup file, have you identified any other backup file that had an access time that did not match the date-modified time and date-created time?

A. No, I did not.

MR. LAROCHE: Let's go to the next slide.

Q. I want to talk about some more activities that happened during the reversion. See the third sub-bullet there?

A. Yes, I do.

Q. What does that convey?

A. This is talking about some more activities that the defendant performed on the ESXi server using that SSH session from the 15th.

MR. LAROCHE: Let's take a look at that.

Let's go to the next slide, please.

Q. What is this exhibit from?

A. This is from unallocated space from the Ubuntu virtual machine on the defendant's DevLAN workstation.

Q. And what command was run by the defendant?

A. This is another LS-ALTR command.

Q. Is this the same log folder that he listed files before?

A. Yes, it is.

Q. And when he listed files before, what was the total log files, approximately?

A. I believe it was 28,000.

Q. And what is the total log files from this list command?

A. It's 30,000.

Q. Were you able to determine at the approximate time this list command was run?

A. Yes, I was.

MR. LAROCHE: Let's go to the next slide.

Q. What is this showing?

A. This is showing the end, the bottom of that list command. I'll explain --

THE WITNESS: Can we go back to the previous slide?

MR. LAROCHE: Sure. Let's go back to the previous slide.

A. So, the -- I just want to explain the last two flags for those commands. We haven't discussed them yet.

So, we discussed previously that when you use the list command with the A flag it shows you all the files in the directory. The L flag shows you details for those files, things like time stamps, permissions, things like that. The T flag sorts those in time order by modified time. And the R flag just reverses that sort. So when you run the command in this way, everything at the bottom of that command is going to be the most recently modified files kind of all lumped together.

OK. You can go to the next slide.

So, this is showing the end of that command with all of the most recently modified files. And we can see from, like, VPXA log specifically, the time stamp that this LS command was run, based on the modified time, is at 5:55 p.m. on April 20.

Q. Now, you see that there's a number of log files that are listed on the right, VPXA, syslog, storagerm, RHTTP proxy, host D, hostd-probe, is that correct?

A. Yes.

MR. LAROCHE: Let's take a look at what happens next on the system, if we can go to the next slide.

Q. So, he had just conducted the list command at approximately 5:55 p.m., is that correct?

A. That's correct.

Q. Let's take a look at what happens next. Is this another log file from the unallocated space?

A. Yes, it is.

Q. And is this a continuation of the unallocated space from the previous slide?

A. Yes, it is.

Q. And how do you know that?

A. Well, we can see here, right above -- it's been cropped.

Oh, OK. Sorry. Oh, it's doing it again.

Q. That's all right. We're fine.

A. Go ahead.

Q. Just look at your hard copy.

A. Well, what slide is this?

Q. It's 132.

A. OK. Just a second.

OK. Apologies.

If you look at the host D probe, what we can see, that that file modified time is 5:55 p.m., so the command was run sometime after this.

Q. And what's the next command that was run after the list command?

A. This command that you can see it on the far right, it's this RM space vpxa.log.

Q. What is the RM command?

A. The RM command, in Linux, is essentially the delete command. So this just says delete the file named vpxa.log.

MR. LAROCHE: Look at the commands immediately after the RM vpxa.log command, if we can go to the next slide.

Q. What are the next set of commands run by the defendant?

A. These are more file-deletion commands.

Q. Can you walk through these?

A. Yes, I can.

Here, we have the first six: RM vmauthd, syslog, storage RM, RHTTP proxy, host D. And then the sixth one is host-probe.

Immediately after host-probe, we get an error from the RM command. If you remember from a slide ago, there's -- there's not a file in that folder actually called host-probe. This is likely a typo. It should be hostd-probe.

And then there's three more deletions after for SDRS injector, VMK warning and VM kernel.

Q. Generally speaking, what are some of the things that these log files would show?

A. So, as we can see, especially from the frequency that these files are updated, these files contain pretty much all the core system logs for the ESXi server. So this would show you things like activities that are happening to virtual machines, whether they're turned on and off; maybe some, like, hardware-level networking information; devices connected to the server. We've seen a lot of events from the host D log, when we look at log-in events from the vSphere or vCenter services. This is the bulk of all of the auditing for the ESXi server.

Q. Would those types of logs be of assistance to you in reviewing forensic materials?

A. Yes, it would be very helpful.

Q. Why?

A. 'cause it contains a lot of -- well, almost all of the auditing information that we have for what happened on the server. And without that, we have to try and recover fragments of these log files from places like unallocated space.

Q. Do you see on the bottom there's a deletion for vmkernel.log?

A. That's correct.

MR. LAROCHE: Let's go to the next command that's run. Slide 134.

Q. Do you see that VM kernel deletion at the top of this slide?

A. Yes, I do.

Q. What's the next command that's run?

A. Another list command with the same flags we discussed earlier, the ALTR flags.

Q. What is the total for this list command?

A. The total is 17,413.

Q. Is that different from the total from the previous list command?

A. Yes. It's a little over half as much.

Q. Why?

A. Because, as we can see from the previous two commands, a lot of files were deleted from this folder, so when LS is reporting the estimated file size for the folder, it's going to be significantly lower since a lot of files were deleted.

MR. LAROCHE: Let's go to the next slide and look at some of the command output for that list.

Q. Did this command, list command, complete?

A. It did not complete. The portion of unallocated space had, one of the blocks that was contiguous in this piece of space that was recovered had been reassigned to a different part of the operating system or a file. So, you can see all the strange characters at the very bottom; it's just showing that part of this command is missing.

MR. LAROCHE: And let's go to the next slide.

Q. Is this another portion of the unallocated space?

A. Yes.

Q. And is this a similar list command to the one we just saw?

A. Yeah. It's not the exact same command. It's a command that was run shortly after the last command.

Q. And does this command complete?

A. Yes, it does.

MR. LAROCHE: Let's go to the next slide.

Q. And what is this showing?

A. This is just showing the end of the output of that list command.

Q. So the end of the output shows the most recent logs created, correct?

A. That's correct.

Q. Where are the log files that the defendant deleted several slides ago?

A. They're not here.

Q. Why not?

A. They were deleted.

Q. At what time, approximately, was this list command run?

A. About 5:57 p.m.

Q. Do you see in the highlighted text the third line from the bottom has hostd-probe?

A. Yes.

Q. Why is that there?

A. That's there because as we saw in the list of deletion commands, the defendant attempted to delete host-probe, where the correct file name was hostd-probe.

MR. LAROCHE: Let's go to the next slide, slide 138.

Q. Does this slide summarize some of the activities during the reversion?

A. Yes, it does.

Q. And the bottom bullet, does that reflect the last list command we just saw that you spoke about?

A. Yes, it does.

Q. Let's look at some additional commands that were run that night. Is this another file from unallocated space?

A. Yes, it is.

Q. And what is this showing?

A. This is showing three more file deletions on the ESXi server.

Q. What files were deleted?

A. The VPXA.0, VPXA.1 and VPXA.2.

MR. LAROCHE: And let's go back to 137 for a moment.

Q. This is the list command that we just saw that was run at approximately 5:57 p.m. Is that right?

A. That's correct.

Q. Are those VPXA logs on this list?

A. Yes, they are.

MR. LAROCHE: Let's go back to slide 139.

Q. At approximately what time did the defendant delete these VPXA logs?

A. Sometime after 5:57 p.m.

Q. How do you know it was after 5:57 p.m.?

A. If we look at the top line of this snip here, we can see that the shell.log from that last list command was last edited at 5:57 p.m.

MR. LAROCHE: Let's go to the next slide.

Q. We talked earlier about VI client logs. Do you remember that?

A. Yes, I do.

Q. What were some of the things we saw from the VI client logs on April 20?

A. The VI client logs had snapshot-reversion history, snapshot deletion, listing of snapshots, log-ins, things like that.

Q. And whose VI client logs were they?

A. They were the defendant's VI client logs.

Q. Now, is this a portion of the VI client logs?

A. This here? No, this is not.

Q. What is this?

A. This is from unallocated space from the defendant's virtual machine on his DevLAN workstation, and this specifically is the recovered session from his SSH session from April 15.

MR. LAROCHE: Let's take a look at the top of the highlighted text, if we could zoom in on that.

Q. You said this was recovered from the administrative session on the server, correct?

A. That's correct.

Q. What does this command reflect?

A. So, this is a command that we haven't seen yet, so I'll explain it.

So, this is the find command. It's a command in Linux that's used to search for files. In this case we're searching for files by the name of the file.

This little slash here after the find command is just specifying the directory on which you want to search for files, and a single forward slash with nothing after it, in Linux, just says, like, search the root of the file system. So, on, like, your Windows machine, you might be familiar with the C drive. Slash on a Linux machine is essentially like the C drive of a Linux machine.

The argument that's given to the name flag is the file name you want to search for, and you're able to use things like wildcards if you may not know the entire name of the file. So we see VI client dash star, the little asterisk. That star is a wildcard, meaning if you find a file that's called, like, VI client-1 or VI client-2, those would all be captured with that wildcard command.

Q. And where was the defendant searching for the VI client log?

A. At the root of the file system. Another way to say that would be search everywhere on the whole server for things that are called this.

Q. On the server itself, is that correct?

A. Yeah, on the ESXi server.

Q. What was the output of this command?

A. We can see directly below it didn't return any results, so it wasn't able to find any files.

Q. Why wouldn't it return any results?

A. Well, if it was unable to find any files with that name, it would return no results.

Q. And are there VI client logs on the server itself?

A. No, there's not client logs on the server. You'll only find client logs, especially client logs that are named VI client, on a client machine, like the defendant's workstation.

MR. LAROCHE: Let's look at the next command that's run. If we could just zoom in on the bottom. Yup. From there down, please.

Q. What's the next command that's run?

A. So, the next command that's run is the same command as before, except instead of searching on the whole file system, we're only going to search in, like, this specific folder for VI client logs.

Q. And again, were there any results to this command?

A. No, there were not.

Q. Why not?

A. Because there weren't any VI client logs found in that folder.

MR. LAROCHE: Let's go to the next slide.

I'm sorry. Let's just go back up one slide for a moment and just zoom in on the bottom few lines there.

THE WITNESS: That would slide 140. OK.

Q. Just focusing you on the bottom where it has an LS command, do you see that on the bottom on 140?

A. Yes, I do.

Q. Where is that command being run?

A. That command's being run on the ESXi server.

Q. And where particularly is the defendant trying to list files?

A. Oh, a directory called /var/log/VMware/journal.

MR. LAROCHE: Let's go back to the next slide.

Q. Do you see that same list command at the top of this exhibit?

A. Yes, I do.

Q. And what's the next command that's run by the defendant?

A. This is another find command, searching on slash, which is the root of the server.

In this case, if you look at the name flag and then the actual file name that's given, in parentheses, it's exactly the same except for the dash is omitted, so this just says is anything -- look for any files starting with VI client.

Q. And what's the next command after that VI client search?

A. It's the same command run again.

MR. LAROCHE: Let's go to the next slide, please.

Q. What is this exhibit showing?

A. This is showing another LS ALTR list command.

Q. And where was this list command run?

A. On the ESXi server.

Q. And what is the total from this list command?

A. 16,529.

Q. And we just looked at a list command several slides ago that had log files in the range of 17,000, is that right?

A. That's correct.

Q. Why is this list total lower?

A. More of those vpxa.0, dot 1, dot 2 files were removed, so this is reflecting that.

MR. LAROCHE: Let's go to the next slide.

Q. What is this showing?

A. This is showing the output from that command, the LS command on the previous slide.

Q. And where do those VPXA 0, VPXA 1 and VPXA 2 logs appear on this output?

A. They're not on the output.

Q. Why not?

A. Because they were deleted.

Q. At what time, approximately, was this list command run?

A. About 6:16 p.m.

Q. How do you know that?

A. If you look at the very bottom, you'll see this dot. We discussed it briefly yesterday. The dot, like a period, in Linux, in the folder structure, represents the current directory. And the modification time stamp of that directory is updated when files are added or removed from the directory. So that dot was updated the last time a file was removed, which was when those VPXA 0, 1, 2s were deleted.

Q. And what's the next command that's run on this slide?

A. So, this is another find command. This is a different thing that we're searching for. Instead of, like, looking for files of a certain name, this dash-newer flag says look at a specific file and find me all files that are -- that have been modified more recently than that file, so find me newer files than this one.

The file that's given to this is this vmksummary.log file, and if you look at the time stamp for the modified time for that log file, you'll see it's UTC 2100 hours, which is 5 p.m. EST. So this just says show me all files on the server that have been modified since 5 p.m. April 20, EST.

Q. At what time did the defendant revert the system?

A. The system was reverted about 5:35 p.m.

MR. LAROCHE: Go to the next slide, please.

Q. What is this exhibit showing?

A. This is showing another list command and a file deletion after that list command.

Q. Let's start with the list command. What is the total log files from that list command?

A. It's 16,529.

Q. And at what time was this list command run, approximately?

A. About 6:16 p.m.

MR. LAROCHE: Let's zoom in on the bottom part of this exhibit.

Q. After the list command was run, what was the next thing the defendant did?

A. The defendant deleted the hostd-probe log.

Q. How do you know that?

A. We see an RM, a remove command, for that log file.

MR. LAROCHE: Let's go to the next slide.

Q. Do you see the top highlighted text there?

A. Yes, I do.

Q. And that shows the removal that you just testified about, is that correct?

A. That's correct.

Q. What's the next command the defendant runs?

A. Another list command, sorted by time.

Q. And what's the total now for log files?

A. It's a little lower. It's 15,891.

Q. And why is it lower?

A. It's lower because that hostd-probe file was deleted.

MR. LAROCHE: Let's go to the next slide.

And the next slide, please, 147.

Q. What is this slide meant to convey?

A. This is just an overview of what we've been talking about, about the defendant deleting different log files and some of the file-size changes for the directory in which he deleted those logs.

Q. Now, the log files that he's been deleting, where have they been located?

A. So, all of these log files have been on the ESXi server in that main log folder for the server itself, not specific to any of the virtual machines on the server.

Q. You talked about different logs being created for virtual machines, is that right?

A. That's correct.

MR. LAROCHE: Let's go to the next slide.

Q. Let's start on the top command here. First, where is this exhibit from?

A. This exhibit is from the unallocated space from the Ubuntu virtual machine on the defendant's workstation, the same spot we've been getting all the rest of this activity.

Q. And at the top there's a root@OSB and at the end an RM vmware.log?

A. That's correct.

Q. What is that showing?

A. This is just showing that a log filed called vmware.log is being deleted.

There's an important thing to note here. If you look just to the left of the RM command, you'll see that our folder has changed, so we're no longer in that main folder for ESXi. We've moved to the folder for his Confluence virtual machine, and inside that folder, that's where logs specific to that VM are stored.

Q. What is vmware.log?

A. We've seen it previously in the presentation. It stores information related to activities on that virtual machine. I think the most recent example was when we looked at that USB device activity from the defendant's virtual machine. That's the type of thing that's stored in the log file.

Q. After the defendant deleted vmware.log, what's the next command he ran?

A. A list command that shows the contents of this Confluence folder.

Q. Approximately when were these commands run by the defendant?

A. We can't date them on this slide specifically. Lower down -- well, I take that back.

At the last line we can see the date for the time that that deletion happened, which was 6:38 p.m.

MR. LAROCHE: So let's focus on that, I guess, last four lines. If we could zoom in, please.

Q. Is this another list command?

A. Yes, it is.

Q. And where is he running this list command?

A. He's running the list command still inside the Confluence virtual machine folder on the ESXi server.

Q. And what's the total?

A. So, the total is the estimated, like, approximate file size for all the files in this folder. You'll notice that the number's a lot larger than it was in the previous slides for the logs for the ESXi server, and that's because for the Confluence virtual machine, this stores the actual -- the actual machine. So there's a virtual hard disk here. There's memory for the machine. And then there's the snapshots, which all have to have all of the state for their own snapshot about what happens. Those are quite large. And then, of course, the log files for the server.

MR. LAROCHE: Let's go to the next slide.

Q. Is this showing the output from that LS command?

A. Yes, it is.

Q. Now, the defendant appeared to run another list command on this slide, is that correct?

A. That's correct.

Q. Now, what's the total from that list command?

A. You'll notice it's -- it starts with 405 instead of the previous total, which was 422, which we can see at the top here. It's been -- it's, you know, significantly reduced in size.

Q. What caused the large deletion of files?

A. This is when that snapshot 3 was deleted.

MR. LAROCHE: Let's take a look at that. Go to the next slide.

Q. Now, we're back looking at the VI client log, is that correct?

A. That's correct.

Q. Were these the types of VI client logs the defendant was searching for on the server?

A. Yes. Yes, it was.

Q. And remind us. Where was this log recovered from?

A. This was recovered from the defendant's DevLAN workstation.

Q. And what does this log show?

A. This is that -- I believe we looked at it earlier. This is showing the prompt that the defendant received when he was going to delete that snapshot-3 snapshot, which was the BKUP snapshot, at 6:55 p.m. on April 20.

MR. LAROCHE: Let's go to the next slide.

Q. Where is this exhibit from?

A. This is from the unallocated space from the Ubuntu virtual machine on the defendant's DevLAN workstation showing that administrative session to the ESXi server itself.

Q. And what command is run on this screen?

A. Another list command.

Q. And the total is still at 405, that long number, is that correct?

A. Yes.

Q. What are some of the things that this list command shows?

A. So, this shows all the files in that folder. You'll notice that the dot file, like we discussed when files are added or removed from the folder gets the time stamps updated -- you'll notice it said 6:55 p.m. You'll also notice that there's no snapshot 3. There's just snapshot 1 and snapshot 2. And then, of course, the file size changed, so we know that this is just confirming that that third snapshot was deleted.

MR. LAROCHE: Let's go to the next slide, please.

Q. What is this slide meant to convey, just focusing on the bolded bullets there?

A. Yeah, the first and last bolded bullets are just showing that that snapshot was deleted, and we can just confirm it based on the file size from the list commands that were run.

MR. LAROCHE: Let's look at some of the more unallocated space. Can we go to the next slide.

Q. What command is run at the top of this slide?

A. It's another LS command. I think it's the same one from the last slide, just showing the full output.

Q. At approximately what time was this command run?

A. 6:55 p.m.

Q. After running this list command, what did the defendant do?

A. If you look at the last two lines here -- I'll draw a line; box them off -- he deleted two VMware log files.

Q. And where did he delete those from?

A. The Confluence virtual machine directory.

Q. Now, I think you testified, several slides ago, the defendant had already deleted vmware.log from Confluence, is that right?

A. Yes, he did.

Q. Why did he do it again?

A. Well, if you look at the file output, there's another VMware log file there.

Q. Why was there a regenerated vmware.log?

A. So, you'll see all these in other cases too -- specifically, we'll look at the VMware logs. You see how they're labeled, like, five, six, seven, eight, nine? That's a feature of -- most Linux servers have something that's called log rotation. Now, what causes log rotation is different based on the service that's performing it, but in this case, for the VMware log specifically, the VMware log is rotated out and archived as one of these numbered versions and then the original, like, non-numbered version is there with the most recent stuff. It's rotated out any time a virtual machine power state is changed, and when you revert to a snapshot, it affects the power state of the virtual machine and causes this log-rotation event to happen, which regenerates, in this case, the vmware.log file.

Q. If you could just circle the time stamps for the vmware-9 and vmware.log on this slide.

A. Try again.

I think that's the best I can do.

Q. And what are those approximate time stamps?

A. That's the last time that log file is modified. One's at 6:51 and one's at 6:38.

Q. And are those the two log files the defendant deleted?

A. That's correct.

Q. If you go above vmware-9 log. And just the next time stamp above that?

A. Yes. This is the April 16 time stamp.

Q. And so that's not even on April 20, is that correct?

A. No. It's from before.

MR. LAROCHE: Understood. Let's go to the next slide, please.

Q. At the top of this slide, you see the deletion for vmware.log?

A. That's correct.

Q. What's the next command that's run?

A. It's another list command.

Q. And is that total different than from the previous slide?

A. Yes, it is.

Q. Is it lower?

A. Yeah, it's lower.

Q. Why?

A. Because the vmware.log and vmware-9 log were deleted.

MR. LAROCHE: Let's go to the next slide.

Q. And is this just a summary of some of the things that you just testified about?

A. Yes, I did.

Q. Let's keep going through the unallocated space. At the top of this, there's the removal for the hostd-probe.log. Do you remember testifying to that earlier?

A. Yes, I do.

Q. Did the defendant run a list command after that?

A. Yes, he did.

Q. And what was the total there?

A. 15,891.

Q. And approximately when did he run that list command?

A. At 6:58 p.m. The time stamp for the file's probably on the next slide.

Q. Let's take a look at the next slide.

A. You can see that here.

Q. And where was this list command run?

A. So, we're back in the log folder for the ESXi server, so not the Confluence virtual machine.

Q. And do you see the next log there?

A. The vmware.log here?

Q. Yes.

A. Yes.

Q. What's the next command the defendant ran?

A. He deletes the vmware.log file for the ESXi server.

Q. Is this a different VMware log than what the defendant deleted earlier that night?

A. Yes, it is.

Each virtual machine will have their own file called vmware.log. This is essentially, like, the master VMware for the whole server.

Q. After the defendant deleted the vmware.log, what is the next command he ran?

A. He ran another find command to look for files newer than shell.log.

Q. And again, what does shell.log show?

A. Shell.log shows commands that were entered into the ESXi server.

Q. Did you see evidence that part of the shell.log were deleted?

A. Yes, I did.

Q. What did you see?

A. The activity from April 20 was deleted and all the activity from the 18th was deleted.

MR. LAROCHE: Let's go to the next slide, please.

Q. The title of this slide is "Badge records." What's the first bullet conveying there?

A. This is just the last time that VMware folder -- I'm sorry, file that we just looked at was deleted, at 6:58 p.m.

Q. Now, there's an excerpt at the bottom there. Do you see that?

A. Yes, I do.

Q. What's that from?

A. This is an entry from the badge records from the CCI office.

Q. And what do those badge records reflect?

A. They show when employee's badged into the building and left the building through the turnstiles or one of the, like, guard gates. And it also shows when employees unlocked vaults for the day. So, you have to go in and put your PIN in and disarm the alarm system, and then similarly, when you would arm the alarm system and lock the vault at the end of the day.

Q. At what point would you lock the vault?

A. You'd lock the vault when you're the last employee to leave that vault for the day.

MR. LAROCHE: Let's take a look, if we can zoom in on this portion of the badge records.

Q. Who is this a badge record for?

A. This is a badge record for the defendant.

Q. And what does it show?

A. This shows that -- this is a close action, meaning the system was armed and that the PIN and, like, password to perform the arming action was accepted. So this, in layman's terms, this says that the defendant closed the vault on April 20 at 7:07 p.m.

MR. LAROCHE: Let's zoom out again.

OK. Let's go to the next slide.

Q. We've talked about a lot of activities on April 20. I'd like to review some of those with you. What are some of the things that happened before the defendant reverted Confluence?

A. So, before Confluence was reverted, at 5:18, Rufus, another employee, his project key, which was in defendant's home folder on the file server, was accessed.

A minute after that the defendant connected a San Disk USB to his Ubuntu VM on his workstation. And at 5:29 p.m., the defendant created a new snapshot for Confluence titled "BKUP."

MR. LAROCHE: Now let's go to the next slide.

Q. What are some of the things that happened between 5:30 and 7:00 p.m.?

A. At 5:35 p.m., the defendant reverted the Confluence server back to that 4/16 snapshot.

From 5:35 to 6:51, the Confluence VM remained reverted, so that's a little over an hour.

Between 5:42 and '43, that backup was the Confluence SQL file and the TAR.GZ file, were accessed from the Altabackup.

And from 5:55 to 6:58, the defendant also deleted various log files from the ESXi server and the Confluence log folder.

Q. And finally, slide 161. What are some of the other things that happened on April 20?

A. So, towards the end of that hour period, the defendant reverted back to that BKUP snapshot that he made. He then deleted that BKUP snapshot, which erases all the activity of what happened on the machine. And then he deleted the --

Lost my screen again. Just a second.

OK. It's back.

At 6:58, he deleted the vmware.log from the ESXi server log folder, and then he locked and left the vault.

MR. LAROCHE: Let's go to slide 162.

Q. Now, you talked about various logs that were deleted by the defendant on April 20, 2016?

A. Yes, I did.

Q. Now, the first bullet says "from the ESXi server folder," is that correct?

A. That's correct.

Q. Does that list out those various log files that were deleted?

A. Yes, it does.

Q. And then down at the bottom there's a bullet, "from the Confluence folder," is that right?

A. That's correct.

Q. Does that list the various files the defendant deleted from the Confluence folder?

A. Yes, it does.

Q. Let's talk about some of those log files. What types of things would the VMware log show?

A. So, the VMware log shows logs related to the operation of virtual machines on the server, so if there were power-state changes made to the VMs, like turned on or off or things connected to them, that would be in the VMware log.

Q. What about VM kernel?

A. The kernel log shows, like, low-level information for the server, like device discovery, storage information, networking and driver information. It also shows some information for when virtual machines start and stop.

Q. What does device discovery mean?

A. So, device discovery, if you remember from the log file that we were looking at, that showed the USB plugged in, that's essentially like a device discovery.

Q. Are those external devices; is that the type of thing?

A. Typically, yes.

Q. What about host D?

A. Host D is -- it's a service log, showing communication between that vSphere server and the VI client server, so this shows when clients are logging in and out of the vSphere application.

Q. And Syslog?

A. Syslog has more service logs, so these are, like, changes that are made to the server.

MR. LAROCHE: Let's go to the next slide.

Q. What about storagerm logs; what would those show?

A. The storagerm logs are just data-storage logs, so things happening to the data storer's storage information server, things like that.

Q. What about the next bullet?

A. The RHTTP proxy shows there's -- sorry. My screen went out for a second.

It shows if there's any HTTP, which is essentially, like, web-traffic, connections that are proxied on behalf of other services. This is kind of, like, lower-level network jargon just to say -- it's just some logging information about how the web service is running.

Q. And VPXA, what would those logs show?

A. VPXA has vCenter-specific logs.

MR. LAROCHE: And let's go to the next slide.

Q. What about the first bullet; what would those logs show?

A. The SDRS injector logs are more data storage-related logs.

Q. And hostd-probe?

A. That's more most host management logs. This one's more of, like, a heartbeat kind of responsiveness checker, so it just kind of makes sure the service is up.

Q. And VMK warning?

A. The warning log shows, like, alert messages and warnings for the server.

MR. LAROCHE: And let's go to the next slide.

Q. Let's talk about VMware for the Confluence folder that was deleted.

A. Sure.

Q. What types of things would that log show?

A. So, as we discussed several times previously, pretty much anything that happens to the virtual machine itself gets stored in the VMware log file. So, when it gets turned on and off; snapshots are made; some, like, data-transfer information sometimes, based on how that was done; things connected to the VM.

MR. LAROCHE: Let's go to the next slide.

Q. Now, earlier you testified that the defendant connected a

San Disk USB device on April 20, 2016, at around 5:19 p.m., is that correct?

A. Yes. Give me a second. I've got to --

Q. Sure. We're on slide 167.

A. 167? 167?

Q. Yes.

A. OK. I'm here.

Q. And this is the San Disk device that was connected on April 20, is that correct?

A. Yes, it is.

Q. And was that before the reversion?

A. April 20?

Q. Yes.

A. It was connected right before, a few -- like, ten minutes before.

Q. Right. Have you reviewed an image of that USB device?

A. Yes, I have.

Q. What, if anything, does that image of that USB device show?

A. It shows that it was formatted on April 21.

(Continued on next page)

Q. Let's go to the next slide, please. There is an excerpt I think from this image; is that correct?

A. That's correct.

Q. Can we just zoom in on that. What does to mean to be formatted?

A. So, formatted can be simply, you're essentially like erasing data on the disc to use it with something else. So, on a Windows machine, you plug a flash drive in and you right click on it in Windows Explorer and you can click "format." It just changes up and updates the file system on the disc.

Q. At what time was this formatted?

A. So, this device was formatted on April 21, 2016, at about 11:46 a.m.

MR. LAROCHE: Your Honor, this would be a good time to break if we can.

THE COURT: We'll take our morning recess.

(Jury excused)

(Continued on next page)

MR. ZAS: Your Honor, can I make a request. Can we get an extra 10 minute on this break. We didn't get a chance to talk to Mr. Schulte about some of this testimony yesterday, so we'd like to spend a few minutes in pens just before we resume.

THE COURT: All right.

MR. ZAS: Thank you, sir.

(Recess)

(Continued on next page)

(In open court; jury present)

THE COURT: All right, Mr. Laroche.

MR. LAROCHE: Thank you, your Honor. Ms. Hurst, if we could briefly go back to slide 26, please.

THE COURT: What slide?

MR. LAROCHE: 26.

BY MR. LAROCHE:

Q. We've obviously seen this slide several times; is that correct?

A. That's correct.

Q. I just want to ask you a question about the tgz files.

A. Sure.

Q. Is that a type of zip file?

A. Yes, it is.

Q. Just generally, what does that mean?

A. So, tgz stands for a G zip tarball file. A G zip is a type of zip compression, and a tarball is way to represent like multiple files as one file. It's a command that you run. We saw it when -- excuse me. We saw it when we went over the backup script. It essentially like zips up the whole home directory into a single file.

Q. So the Confluence tgz file, fair to say Confluence would be larger when unzipped?

A. Yes, it would.

Q. Let's look at the next slide, 27. Is this reflecting Stash backups?

A. That's correct.

Q. We talked about this yesterday a little bit.

A. Yes.

Q. How big approximately is the tgz or tar file for a Stash backup?

A. The zipped backup is over 200 gigabytes. It's quite large.

Q. As an unzipped file, approximately how large would that be?

A. It's bigger. I don't remember exactly how large. It's been a while since I've unzipped one, but less than 500 gigs.

Q. Thank you. Let's go back up to slide 169, please. I want to switch gears a little bit to talk about the tool Brutal Kangaroo. So let's go to the next slide.

You remember yesterday we saw some of these audit log files for Brutal Kangaroo? Do you recall that?

A. Yes, I do.

Q. Are these the same types of audit log files?

A. Yes, they are.

Q. So let's just walk through these. What is the top file showing?

A. This is showing a permission, project permission granted event for project admin. I'm sorry. I'm drawing all over myself. For the defendant from Dave.

Q. So Dave was giving the defendant admin access to Brutal Kangaroo?

A. Yes.

Q. When approximately did that happen?

A. This was at about 1:03 p.m. on May 26.

Q. What about the bottom log file, what does that show?

A. So, at 1:33 p.m., the defendant modified and removed permissions for the user Christopher from Brutal Kangaroo.

Q. 1:33 p.m. on the same day?

A. That's correct.

Q. Let's go to the next slide, please. Is this another audit log file?

A. Yes, it is.

Q. What does this reflect?

A. So this is showing that the defendant, and this is his IP address, is making an update to the status of different branches of the Brutal Kangaroo project. Specifically, this Brutal Kangaroo project had two branches, a develop branch and a master branch. I'll explain that briefly.

So in computer programming, like, software development in a team of people, you'll have -- there's different ways you can go about doing it, different kind of industry standard practices. But in the case we're going to talk about here, you'll have two different branches of code. So you'll have two different places where your code will live. You'll have the master branch, where you only push like working solid versions, so that's your version 1.2, your 1.3, version 2.0 software.

And you'll have another branch where you do development in the meantime.

The reason you do that is so that no one pushes code to the master branch that could potentially break what users down the line are using.

In previous testimony, we've heard the, like, follow the pull request model. That's how you would push code into these branches, and it gets usually peer reviewed to make sure that those kind of changes wouldn't happen.

Q. So what is this log file showing?

A. This is showing these two branches are having their status updated to read only from like a read write state. Just meaning that the project's kind of frozen so no one can contribute to it.

Q. Let's go to the next slide, please. Is this more log files relating to Brutal Kangaroo?

A. Yes, it is.

Q. What does this activity show?

A. This is showing the defendant from his IP address removing permissions, specifically write permissions from a specific group, and that group is the sg-OSB group.

Q. So this is showing a removal of permissions; is that correct?

A. Yeah, the permissions being removed.

Q. Did you see any audit logs reflecting the defendant giving

anyone else access to Brutal Kangaroo?
A. Giving access? No, he removed access for these projects.
Q. Did you see any evidence of him giving access back?
A. I don't believe so.
Q. Let's go to the next slide. The last part of your testimony is about the leak itself.
A. That's correct.
Q. You stated earlier as part of your investigation you reviewed the Vault 7 and Vault 8 disclosures by WikiLeaks; is that right?
A. Yes, I have.
Q. I want to focus on March 7, 2017. That disclosure. Do you have an understanding about where that information came from on DevLAN network?
A. Yes, I do.
Q. How do you know that?
A. I've reviewed both the content of the leak and content from backups on the DevLAN network.
Q. Where did that content come from?
A. It came from Confluence.
Q. How much of Confluence, approximately, was disclosed on March 7, 2017?
A. All of the page contents and attachments, things like that.
Q. Let's go to the next slide, please. Based on your investigation in this case, have you identified potential ways

in which an individual could obtain all of Confluence from DevLAN?

A. Yes, I have.

Q. What are some of those ways?

A. So there's three main ways that you can go about taking data from Confluence if you wanted to walk out with it.

The first is what we call a web scrape. The second would be taking the whole Confluence virtual machine from the server. And the third would be to take the backup files from Altabackup.

Q. Let's walk through each of those. What do you mean by a web scrape of Confluence?

A. So, in computer science and computer security terms, scraping a website can mean anything from like taking the screenshot of it to making a, like, lower-level request, like from the command line to retrieve like the source of the page.

And what we mean by this method would be someone would over time, either by manually going to every single page, they would take a screenshot, or Confluence actually has a page export function where you could make like a PDF of the page. Either doing that for every single page on the whole server or writing a script to automate that process.

Q. What privileges would you have needed to take a web scrape of all of Confluence on DevLAN?

A. So, for all of Confluence, you would have needed some level of administrative privileges, because you're doing this from, like, your user session through the web browser. And certain pages are restricted to certain users. So you wouldn't be able to view all the pages, unless you had all those permissions.

Q. How long approximately would this method have taken?

A. It's going to vary wildly, depending on what type of method's used. If you are going through every single page, like one at a time, making PDFs, this would be a significant amount of time, because there's thousands of pages.

If you write a script to do the process, it could be completed in any number of days, it just depends on how fast you make requests to the server and how fast it can respond.

Q. Is it your opinion that a web scrape was the way that all of Confluence was taken?

A. No, it's not.

Q. What are some of the reasons for that opinion?

A. Primarily, and we'll see towards the end of this presentation, there's content that was posted on WikiLeaks that appears like on the page that would never appear on the pages as it was displayed to a user on DevLAN.

Q. Let's talk about the second method, copying a virtual machine.

A. Yes, through vSphere, or conversely by copying files directly off of the ESXi server, you can make an export of the Confluence virtual machine. So, you basically, you log into vSphere and you click on the Confluence VM, you right click on it and there's an option that's called something that's usually like export to OVA or OVH. Those are just VMware's name for their appliance export file.

The problem with this is you have to turn the machine off and stop it before you can make this kind of an export. So, for that reason, primarily, and for some other reasons we'll discuss later about page content that was disclosed, I don't think it was taken from the virtual machine like that.

Q. And approximately how large is the Confluence virtual machine?

A. I believe it's about 200 gigabytes.

Q. Is that larger than the backup files?

A. Significantly.

Q. How large was the Confluence backup file approximately?

A. I believe the database was about 400 megs, and I think the home folder was maybe like two and a half gigabyte, something like that.

Q. Let's talk about the third method on the screen. Copying the Confluence backup files.

A. Yes.

Q. How would someone do that?

A. So the Confluence back up files were in two places. They were on the Confluence server itself in this dot, hidden dot backup folder, and they were also on the file share on the

NetApp in the Altabackups folder.

Q. How would someone copy it from those folders?

A. You would need a location that had the Altabackup server mounted, or it would be inside in this case for Confluence, inside the Confluence server itself, to copy off of those backup files.

Q. You mentioned two files that were in the Altabackup folders, the SQL file and the tarball file?

A. That's correct.

Q. Would you need both of those files?

A. Yes, would you need.

Q. Why?

A. So, as we'll see later on, there's content -- the SQL database contains a lot of the page content information for the Confluence service. But, the home folder zipped file has things like all the attachments for the pages, server configuration, information, things like that.

Q. Is it your opinion that taking these Confluence backup files was the way that all of Confluence was stolen from DevLAN?

A. Yes, it is.

Q. What are some of the reasons for that opinion?

A. Namely, they mostly pertain to elements that we can see in the pages on WikiLeaks, and some of the issues that were surrounding the SQL database backup file itself.

Q. Let's talk about that for a second. Issues with the SQL backup file?

A. Yes.

Q. Can we go to the next slide. This is titled "Backup Scripts." Remind us what is a backup script.

A. So a script on Linux is essentially plain text file with a list of commands for the computer to run. So a backup script is a file that's just used to back up data from the Confluence server. These scripts were set up in a fashion on the computer that they would run daily. I believe it was at like 6:25 a.m. every day, the script would run, and would back up the files and push them off to Altabackup.

Q. So let's take a look at one of those scripts. We can go to the next slide. What is this?

A. This is the shell script that does the heavy lifting of creating that zipped up home folder and doing the export from the database.

Q. Where was it located?

A. This is on the Confluence server itself.

Q. Generally, what did this script do?

A. This script takes a few arguments and navigates to the place where Confluence stores its data. And then it names the backup file with the date and the name of the service, in this case Confluence, and it zips up -- I can circle it here. It uses the tar command to create a zip file for the whole home folder for the Confluence service. And then it makes a dump of the SQL database, the MySql database that's storing the rest of the information for the service.

Q. Was there an error in this script?

A. There was.

Q. Let's go to the next slide, please. What was the error?

A. So it has to do with the MySql dump command. If you take a look at one of the SQL backups from the Confluence folder on Altabackup, you'll notice in the middle of one of the tables -- so databases are organized into tables and rows inside those tables. So, one of the tables, you'll notice it kind of just stops halfway through, and there's nothing else after it. The reason that happens is there's what we call a character and coding error. Character and coding in computer systems is just a way that the computer translates -- like, if you see, like, if you type the letter A on the screen, the way it translates that letter into binary that the computer can read, there's various different ways it can do that. And if you don't have the data in the database synced up to be storing that data in the same way as, for example, like how you're viewing the system when you're using it, when you do exports such as this and you don't set it to a specific encoding, you can run into certain errors.

And that's just a long way of saying that these backup files all had this error, which meant that about, you know, three-quarters of the way through the process of backing up the database, it hit this error and then stopped. And any tables after that point were not included in the backup. But it still saved the backup up to that point.

Q. What types of tables were missing?

A. The tables that were missing were actually very important tables. They have to do with the user mapping info for user names for different users that were in Confluence to internal database values, which are essentially these long strings of user identifier numbers. So, any, like, it's the main way you would attribute certain users to certain pages and comments, things like that.

Q. Let's go to the next slide. This is titled "Building Confluence Pages from the Altabackup Files." So I'd like to talk about that process for a moment.

What types of things would you have to do to reconstruct the Confluence Altabackup files?

A. Sure. So if you got, if you got these two backup files and they like landed on your desk, the first thing you'd do is you'd look and see what the file name is. So, the backup files were named, they had the word "Confluence" in the name. So a quick Google search of that, you could see it was an Atlassian product. They actually offer like a free trial. And they have instructions on how to restore from backups. Reading that, you would see that these appear to be like the backup files you would need to restore it. And if you put them in and go through the restore process, through like the recommended method from Atlassian, it would fail. And that's because that database is incomplete. So it's unable to completely restore everything.

Q. What do you mean by fail? Like, how would it not complete?

A. It would -- you would try to restore from the backup, and it would -- it just wouldn't work.

Q. So, if that method did not work, how would you reconstruct the database?

A. You would manually have to go into that database file, and the associated home folder, and start reconstructing the data manually.

Q. Let's go to the next slide and talk through that process. How you go about doing it manually. What's one of the first things you would need to know to reconstruct the database manually?

A. First thing you have to know is how data is stored in these backup files. We have two backup files, one is a database and another's, you know, essentially just a zip file of some files and folders.

So, the first thing we'll do is take a look at that database file. The database file has all of the page content that you'd find on a Confluence page. You'd have the order those pages were in, user names, comments on pages, locations on disc to where attachments for pages were.

So if you put a picture on a page, you'd have, like, the path to where that picture is stored. Confluence pages have a concept of page revision history. So you could have, if you have a page that a lot of people are editing over the course of a couple years, it could have like 20 different page revisions. So this is just to go back, if you wanted to view an earlier version or restore if someone deleted something accidently. There's ownership of pages, so certain users might own pages. There is a concept of a space in Confluence which is essentially like a, you think of maybe a project or something like that. Those can own different pages. You have to look through the database and figure out how all these relationships work. Some are easy and some are not.

Q. As part of your work in this case, did you conduct that analysis to figure out how the database stores information?

A. I did.

Q. How long did just that process take for you?

A. Just the process of reviewing the database and figuring out how it worked, I probably spent about a week on it, and I had the benefit of kind of knowing what to look for. Because we had some other analysts who had looked into this in the past.

Q. After you determined how Confluence stored data, what would be the next step in actually constructing the database?

A. Once you know how everything works, and what you want to use out of it, you'd have had to figure out a way to get that into some kind of web page for people to view. Because normally, on a Confluence server, it is going to do all that for you. So you're going to have to figure out how to pull that information out and display it in a useful way.

Q. Would this process have been made more difficult by the fact that the user related tables were not included?

A. Significantly more difficult.

Q. Why?

A. The way that Confluence stores page reference information, it changes some of the values between some of the different tables. And without knowing -- being able to directly map the user identifier numbers back to their space IDs, the page IDs for pages that they created, it can be very difficult to figure out who might have owned a certain page, or, you know, something as simple as what a user's name might have been.

Q. How would you actually reconstruct it after determining all those relationships?

A. The most expedient way and way to do it would be to write a script to parse that database file and create some kind of -- a bunch of HTML pages off that.

Q. Would this process have restored Confluence to the way it appeared on DevLAN?

A. No.

Q. What would be different?

A. There would be significant differences in formatting. There's a lot of dynamic content that Confluence provides. There are a lot of what I'm calling, like, template macro objects in the database on the page. These are like kind of little bits of computer code that the Confluence server sees, and says, oh, okay, this says I need to make a pretty table graphic here and then fill it with this information. So, if you're unable to ascertain how that works, then that's going to be missing. Things like that.

Q. So let's look at some of those differences on the next slide.

Now, the first bullet says "User names are not available." What is that meant to convey?

A. So, this is for talking about things that are missing from the database. Since the user mapping tables with the names of users aren't there, the only way you can glean what a user's name would have really been is from the title of a page. So if a user named their page like "Pat's Home Page," then you could probably assume that Pat was the one who wrote the page.

I think there have been maybe one or two other tables that had a couple of bits and pieces of user information. But the main table where that were stored were not included in the backup.

Q. Did some of the posts by WikiLeaks on March 7 include individuals' names from the agency?

A. Some posts in the body content had names. Most of the names were redacted though.

Q. What do you mean by included it in the content?

A. There were a few pages in the actual, like, main body of the page that had names in it that missed the redaction pass that WikiLeaks ran over it.

Q. Why would those names be available in a SQL database if there was an error in that script?

A. So that would have been something someone would have just manually typed in. And didn't use one of the features to, like, embed a link to that user's page when they referenced the user name.

Q. When you say the content, was the content included in the SQL database?

A. Yes, it was.

Q. So that was not a table that was missing?

A. No, it was not.

Q. So, the third bullet says "No Confluence images, pictures, or other features." What does that refer to?

A. So, we'll see some pictures in some following slides, but, you know the pretty, like, Confluence web page with the title bars and all their pictures, none of that would be available from the database because that's all built by the server.

Q. What about dynamic elements, what is that referring to?

A. So dynamic elements can mean anything from, like, the code that I mentioned that's stored on the page, it has to get executed by the server, to things like, you know, clicking the drop down and changing permissions for pages, or, you know, adding new pages. Things like that.

Q. And page formatting?

A. So, the page formatting itself is going to be drastically different. To some extent, the HTML, like the program language used to design web pages, that's actually stored in the database. So you can pull that content out, and kind of put it in as is, and it will keep the basic structure of how the body content of the page was stored.

We have an example of this. Anything beyond that, like, what color the text should be, how big it should be, what font it should be, how wide should the margins be, things like that, that's not going to be stored there.

Q. Let's take a look at a regular Confluence page from the internet. To be clear, this is not from DevLAN, correct?

A. Yeah, that's correct. This is a picture off of Google.

Q. What's this showing?

A. This is what Confluence looks like when it's running. This kind of shows all of the different buttons you can click, how it -- how like body content for pages looks. When I mentioned those little code elements, so, little boxes like this and this. Tables like this. Those are types of things that you'd have to manually account for when you were reconstructing the database, and it might be very difficult to do.

When I say like dynamic elements, I mean things like what I just showed you as well as obviously, like, buttons to operate on the page, and things like that are not going to be available in your reconstructed version.

Q. Let's take a look at an example from DevLAN itself. Let's look at the next slide. What is this showing?

A. This is a screenshot from one of the Confluence pages on DevLAN. And you can see it's very similar in form factor and layout to the page we were just looking at.

Q. Let's look at some examples of what actually posted to WikiLeaks. What is this exhibit showing?

A. This is showing a page from WikiLeaks that just contains some -- it's a basic page. There is not a whole lot of information on it. I just wanted to show how easy it would have been to pull the basic body content out of the database and make a page of it.

Q. Why would that have been easy with the Confluence backup file?

A. All these things, like the indentation here and the numbers, this little kind of quote block, even some of the spacing some of the, like, title information, things like that. That's stored in the page formatting in the database. So, all you really have to do is copy it out and put it in an HTML file and open it in a web browser, and it will do the rest for you.

Q. Is this an example of where WikiLeaks formatted the body content correctly?

A. To some extent, yes. There -- we call it a style sheet. It essentially is what determines, like, what a web page makes certain colors of text on the page, what font it is. This has the WikiLeaks style sheet applied. That's why this is the same color green as this and this. The text is the same font. Things like that. So they applied their style sheet to it to make it look a little nicer.

But I'll show you as far as formatting perspective that it's pretty much exactly as it was in the database.

Q. Let's look at the next slide. What is this showing?

A. This is just a very simple example. I literally copied the row out of the database that has the body content data for this page and just pasted it into a text file and opened it with a web browser. And it, you can see it formats everything almost in the exact same manner that it's formatted on WikiLeaks.

Q. Sorry. You copied this out of where?

A. Out of the Confluence database backup file.

Q. So the actual backup file that was on DevLAN?

A. Yes.

Q. Let's look at the next slide. Let's compare these two. What is this showing?

A. This is just a side-by-side comparison. You can see that it's, it's identical except for the one I made, I didn't apply any kind of style sheet to it. And the one on WikiLeaks has the WikiLeaks style sheet. So...

Q. Let's go to the next slide. Did other pages posted by WikiLeaks omit information that would have been contained in a full Confluence virtual machine?

A. Yes, they did.

Q. I'm showing you a slide with Government Exhibit 10. Do you see that?

A. Yes.

Q. The title of the slide is "User ID in WikiLeaks Page Contents." Do you see that?

A. Yes, I do.

Q. In what ways is this slide different than how it would have been displayed on DevLAN?

A. This big ff808 number is not something that Confluence would ever like display to a user or even an administrator in the web view, to be honest. This is a number that's used internally in the database to reference other parts of the database and different values.

When WikiLeaks, just having the database was parsing through it, since they couldn't map these numbers back to actual user names, there are pages for certain users who they can only reference by this value. If you searched for this in the Confluence, like, the Confluence web server on DevLAN, you would never see this ff808 number.

Q. Are there different ff808 numbers for different users on Confluence?

A. Yeah, each user has its own unique user identifier number.

Q. Does this page also omit anything else that would have appeared on DevLAN?

A. I think this page specifically, especially the way it's formatted, I don't think this is a page that existed at all. You see how they kind of have a placeholder for assigned spaces? There's, like, no data in it, and assigned pages. This is more like a list of all things that have to do with this user name and less of a construction for that user specifically.

Q. What conclusions, if any, have you drawn from this page as posted on WikiLeaks?

A. I've drawn that they rebuilt this page and the other pages from that Confluence database, SQL database backup file.

Q. Let's go to the next slide, please. This is titled "Incorrect Page Number Association." And it has Government Exhibit 7-1.

A. Yes.

Q. Is this another page from WikiLeaks?

A. Yes, it is.

Q. Is this also from the March 7, 2017, posting?

A. It is.

Q. In what ways is this page different from how it would have been displayed on DevLAN?

A. So, on DevLAN, there's actually no page called MacOS X. That page doesn't exist. What happened, at least my opinion, what I think happened was, when WikiLeaks was going through the database, since they don't have user information, it can be pretty difficult to pin exactly, you know, what page belonged to a specific user. There was a user who happened to work on a lot of Mac related tools. So, naturally, their user space page has a bunch of pages that have to do with MacOS tools. These tools didn't ever belong to like a top-level page called MacOS X. The page they belonged to was the name of the user who made these pages.

So, when WikiLeaks was going through and looking at what was here, they just assumed incorrectly that this was a page that was made for MacOS X notes, not a user's page on notes.

Q. Let's go to the next slide. This is titled "Missing/Deleted Pages." The top exhibit is still Exhibit 7-1. There is a red box around Ghidra; do you see that?

A. Yes.

Q. Why is there a red box around Ghidra?

A. This page is a deleted page. If you browse to the Confluence page for this user on DevLAN, you wouldn't see this Ghidra page. You'd actually have to go as that user into the page, go into the trash can, and, you know, manually restore that page for it to show up.

So, this shows that either on purpose or by accident, WikiLeaks restored deleted pages that were found in the database when they made the dump. Or made the post, excuse me. This page was created on, like, September 16, 2015. I'm sorry. It was created on the 15th and deleted on the 16th, shortly afterwards.

Q. At the bottom there, there is a Government Exhibit 1207-94 that you've been circling.

A. Yes.

Q. Where is that from?

A. So, this is an actual entry from the Confluence, like -- excuse me, that March 3 Confluence SQL database backup file. This is one of the tables. This is specifically a table called "content." This is the SQL query I ran to generate this, by the way. And I was basically searching all pages in the content table for names that were something like Ghidra 6.0.10, and this is the results of that.

Q. Why were you looking at the March 3, 2016 backup file?

A. Because that's the backup file that I believe was posted on WikiLeaks.

Q. Let's go to the next slide, please. This is titled "Missing Template and Design Elements." And it's showing Government Exhibit 8-1. What is this showing?

A. So, I believe this is the last example. Remember when I circled some of those pretty looking tables and, like, colorful entries inside the tables on the site from Google. So, the script that they wrote to rebuild this didn't really account for all of that. Some were accounted for, but others were not.

If we circle this top part here, you see we have the title of this page, and then this detail is missing. The first time I saw, like, a note like that in the page, that's usually kind of indicative of a script having had kind of parsed through this and it was either unable to figure out what was there, or what seems like here, hey, the details for this object aren't there.

But, after taking a look at the SQL database itself, it was clear that the script was just unable to parse this -- "parse" meaning process -- this template macro code thing.

Q. Let's look at that. Let's go to the next slide, please. Now there is an overlay of Government Exhibit 1207-93.

A. Yes.

Q. What's that showing?

A. So, this is from the body content of this page. Like I said before, it is essentially all HTML web page code. And this is what's missing from this details missing section.

Why is it called details? Well the name of this template is called "details," so that's why that's there. And then for whatever reason they couldn't process everything inside here, which is just a small little table. So this would have been a table, kind of similar to this table below, except it just has a date column, and like a participants column. And a date, time and some user names.

This is another good example of this is how a user name is stored in the database. So, even if this were to be reconstructed, they'd have to go and figure out what this ff808 number belonged to, and then either replace it with a user name if they were able to find one, or just leave it as is. This is, this link, when you see this link, that's when Confluence sees that, it says, oh, okay, I need to go resolve this to something that a human can understand.

Q. Let's go to the next slide, please. This is the Confluence Altabackup files; is that correct?

A. Yes, it is.

Q. What impact, if any, did these exhibits have on your opinion that the data provided to WikiLeaks was from backups?

A. So, we know that the date accessed was from 4/20 at 5:42 p.m. and 5:43 p.m. for the two files specifically. And we know that that falls into the activity that we have from the defendant, that was, you know, purposefully reverting to the Confluence virtual machine to a time when he had access to it, doing something for over an hour. These files are accessed during that time. And then shortly after that, all the log files on the ESXi server itself were deleted, the log files for the Confluence server were deleted, and all the activity of that session are gone.

MR. LAROCHE: No further questions. Thank you.

THE COURT: Ms. Shroff.

MS. SHROFF: Thank you, your Honor.

THE COURT: You're welcome.

CROSS-EXAMINATION

BY MS. SHROFF:

Q. Could we pull up, please, Government Exhibit 1203-54.

So you see that line, sir, that starts 2016-04-20T17:19:23. You see that line?

A. Yes.

Q. Okay.

A. The first line here, right?

Q. I don't know if it is the first line. It is the line where I'm starting.

A. Okay.

Q. So, that line, sir, says, if you keep following, right, it says "USB: Found device." Correct?

A. Yes.

Q. And then it has a little bracket. You with me?

A. I believe so, yes.

Q. Okay. Good. Name: And then it says Sandisk. Correct?

A. Yes.

Q. Okay. Then there is a backslash. Extreme vid colon, bunch of numbers, super family storage.

You with me there?

A. Yes, ma'am.

Q. And then there is a whole continued line of numbers, right?

A. That's correct.

Q. And then it says "found device." Right?

A. Correct.

Q. "Found device" means that that's when the USB is found, right?

A. Correct.

Q. Okay. So, then, you see that line that says right above it -- and I think John or Achal will get it for you -- 206-04, you see that?

A. Yes, ma'am.

Q. It keeps going, correct?

A. Hmm-hmm.

Q. You see that line, it still says "USB found device." You with me?

A. Yes.

Q. Okay. I don't do this very often, so just be patient, okay. Then there is a bracket. It says "name," correct?

A. Yes, ma'am.

Q. Then it has this number. T8R2, right?

A. Yes.

Q. You with me?

A. Yes.

Q. Okay. Then it continues, right?
A. Correct.
Q. Okay. So, could you just do me a favor and look at the two numbers. The date, you agree with me, both say 2016?
A. Yes.
Q. And you agree with me both say 04.
A. Yes.
Q. April?
A. Yes.
Q. Okay. Then it says dash, both of them say the same thing, right?
A. Yes.
Q. And then there is a number 20T17:19 on both sides, right?
A. Yes.
Q. And then both sides also say colon 23, correct?
A. Yes.
Q. And then there is a dot. Correct?
A. Yes.
Q. And then there is 441, correct?
A. Yes.
Q. And there is another dot.
A. Yes.
Q. No, no, there is a dash. Don't say yes. That's a dash.
A. Yes, it's a dash.
Q. Dash 04, right?

A. Yes.

Q. And then colon?

A. Yes.

Q. 00?

A. Correct.

Q. Same time to the nanosecond.

A. Yes.

Q. I keep getting this wrong. It's Sandisk, right?

A. Correct.

Q. I keep calling it San. Sandisk, and the right block exactly at the same time to the nanosecond. Correct?

A. Yes.

Q. Okay. Let's just see if we can go down. You with me?

A. Hmm-hmm.

Q. They are going to pull this up for you. 2016-04-20T1722. You with me?

A. Yes, ma'am.

Q. 20907-4?

A. Yes.

Q. What time is that, by the way?

A. 5:22 EST. It has the minus four at the end so you know it's EST.

Q. Keep going. You see that says "USB:found device"?

A. Yes.

Q. You keep following that line it ends with "speed super"?

A. Yes.

Q. Go down, keep continuing. And then it says on the right-hand bottom -- you with me?

A. Yes.

Q. What does it say there?

A. "Disconnected."

Q. "Disconnected:1"?

A. Correct.

Q. Okay. And then gives you a bunch of keys below?

A. That's correct.

Q. This is my exhibit, 1203-54, in its bigger form.

A. Correct.

Q. You showed the jury on your slide deck the same thing, and then you cut off the "disconnected" part.

A. Correct.

Q. What time is that USB disconnected?

A. It was disconnected at 5:22, about three minutes after it was connected.

Q. Let's show them again then, why don't we, the timings of your reversion.

A. Sure.

Q. And then tell me if that USB disc, Sandisk, disconnected before the reversion or not.

A. Oh. Before.

Q. Before the reversion, right?

A. Yes, ma'am.

Q. So it's out?

A. Correct.

Q. Not inserted?

A. Correct.

Q. Taken out?

A. Yes.

Q. You didn't show it to them.

A. It was not --

Q. No, no, no. Right here on the left?

A. Correct.

Q. You showed it to them?

A. Correct.

Q. No.

A. Not the removal, no.

I'm sorry, could you repeat?

Q. You cut it off, did you not, sir, on the left side?

A. Yes. But not intentionally cut off to remove the disconnect.

Q. It's not intentional?

A. No.

Q. Okay. Well, let's talk about that. It's slide 105. Right. Let's put the whole slide in.

Who made the slide?

A. I made the slide.

Q. How many hours did you spend making the slide deck? I'm not talking just about 105. Okay, take your time. Think about it. All of these slide decks.

A. A lot.

Q. Well, you are going have to quantify a lot. A lot means nothing to me. Quantify it.

A. Maybe, let's say, 40 hours over the course of a few months.

Q. 40 hours?

A. Maybe more.

Q. Come on. Really?

A. Probably more?

Q. Let's try it this way.

A. I don't remember specifically.

Q. It's okay, it's okay, we have all day. Don't worry about it. Let's start with when you started work on this case. Remind us, would you?

A. Around March or April 2017.

Q. March or April 2017, right?

A. Correct.

Q. And when you first started, sir, you used the word "deployed." To me that just meant you go somewhere, right? In your case?

A. Correct.

Q. Right. It's not like you are going to the Army, right?

A. No.

Q. Okay. So, you start off and you go to work and you are sent to help the CIA out, correct?

A. That's correct.

Q. You are a contractor for a company?

A. Yes.

Q. I'm sorry. I'm a little confused about that. Are you an employee of the company and contracted to the FBI, or are you an employee of the FBI and contracted to the company?

A. The first one.

Q. So you work for a company?

A. Correct.

Q. The company has a contract with the FBI, correct?

A. Yes, we do.

Q. And then you were sent out to work on this case, and then you presented this unintentionally cut off slide 105?

A. Correct.

Q. Okay. And when you first went there to help them out, you were just sent there not in an expert capacity, right?

A. I disagree.

Q. You were sent there knowing you were going to be hired as an expert to testify in this case?

A. No.

Q. Oh. Okay. So, you were just sent there to work on the case, correct?

A. Correct.

Q. And when you got there in March of 2017, did you realize that the CIA had been unaware of this data given to WikiLeaks for almost a year or did you learn that a year later?

A. I learned it during the investigation.

Q. Okay. And when you were sent off to help these people, were you sent to help the FBI or were you sent to help the CIA or are they the same?

A. I support the FBI. But we were there to help the -- assist the CIA just to determine what happened.

Q. You support the FBI, but you were -- okay. So, you were sent -- did you actually physically go to the CIA?

A. Yes.

Q. And you met with the people at the CIA, correct?

A. Correct.

Q. And when you went there, were you sent along with the FBI agents in this case?

A. No, not the -- well, some of them.

Q. Some of them. How about Special Agent Donaldson over there on the left-hand corner?

A. Not at the beginning.

Q. Not at the beginning?

A. No, ma'am.

Q. How about Special Agent Schlesinger; was he there?

A. Not at the beginning, no.

Q. And how about Special Agent Evanchec; was he there?

A. Yeah, I believe Rick was the first one I'd seen. One of the agents prosecuting the case.

Q. How about somebody named Mr. Berger; was he there?

A. Mr. who?

Q. Mr. Berger?

A. Yes, he was.

Q. He was there, right?

A. Correct.

Q. You started in March of 2017 working with all of these folks from the FBI and the CIA, correct?

A. Not all.

Q. I mean, you know, as the judge said before, it's a phrase. Folks from the FBI?

A. Correct.

Q. Folks from the CIA?

A. Correct.

Q. Okay. Is it fair to say, sir, that from the time of March of 2017, until now, you've never consulted with the defense, correct?

A. That's incorrect.

Q. You've consulted with us or you've given us discovery? Those are two different things. "Consulted" meaning you work with us.

A. Oh, I'm sorry.

Q. Okay.

A. I meant from like a discovery perspective.

Q. No, you never consulted with me, right?

A. No.

Q. I've never sat down, helped you make these slide decks that were inadvertently cut off?

A. No, ma'am.

Q. So, you worked exclusively with the FBI, right, and the CIA?

A. Yes.

Q. You met with them almost weekly for a while, correct?

A. Correct.

Q. You generated weekly reports for them, correct?

A. I did not generate a weekly report for them specifically. But we did as a team gave weekly reports.

Q. Let's talk about this team. Who's on this team?

A. FBI employees and the CIA analysts.

Q. Okay. So all told they're like how many of you, eight, nine, 10? How many were on that e-mail chain; do you remember?

A. E-mail chain?

Q. Hmm-hmm.

A. I'm sorry?

Q. The e-mail chains where you talk about when to meet, how to meet, what we should do next, how we should get ready for the case?

A. We had maybe, I think maybe at its high point 30 different people working in the lab.

Q. Okay. And is it fair to say, sir, that for your company, you generated what is called a monthly report?

A. That's correct.

Q. So every month you would tell them, hey, I'm still working on the CIA case, and this is what I'm doing, right?

A. That's correct.

Q. And there came a point, did there not in this -- it's been two years, right? More?

A. Almost three.

Q. Almost three. So for three years, you've been sending monthly reports telling them you are doing all of this stuff for the CIA on this case?

A. I'm sorry. Could you repeat the question?

Q. Sure. Maybe I'll try and go slower.

You wrote monthly reports each month, yes? And you sent these monthly reports to your company, correct?

A. Hmm-hmm.

Q. Detailing the work you were doing for the CIA. Correct?

A. Correct.

Q. Okay. And you got paid, right?

A. Yes.

Q. And the CIA paid you -- not you directly, but your company, correct?

A. No.

Q. Oh. Then who did the CIA pay?

A. The CIA didn't pay me. I don't work for the CIA.

Q. No, no, I know you don't work for the CIA. You testified you don't work for the CIA. My question is how did your company -- what is your company's name, MITRE?

A. MITRE.

Q. How did MITRE get paid?

A. Well, we're paid from the contract. Specifically in this instance, our contract with the FBI.

Q. Okay. So MITRE is a private company, you provide services to the FBI, and the FBI's working with the CIA. Correct?

A. That's correct.

Q. Do you know by any chance for three years how much MITRE got paid for all of this work?

A. I don't know.

Q. 500,000?

A. I don't work in contracts. I really don't know much about our budget.

Q. Oh, I'm not talking about your budget. I'm talking about how much you got paid. That's not a budget, that's what money's coming in. I'm not asking about money you spent.

THE COURT: You want to know how much MITRE got paid?

MS. SHROFF: Yes.

THE COURT: Do you know?

THE WITNESS: I don't know.

THE COURT: He doesn't know.

Q. MITRE didn't have a contract with the FBI or the United States attorney's office that you know of?

A. We had a contract with the FBI. I don't know the dollar value attached to it.

Q. Okay. And it's fair to say MITRE gets a lot of business from the FBI, right?

A. That's fair.

Q. In fact, would you say that more than 60 percent of the work for that company comes from the FBI?

A. I don't believe that's accurate.

Q. Okay. Now, in addition to the monthly reports, you met with people from the FBI and the CIA on a very regular basis, correct?

A. Correct.

Q. And when you met with them, you had team meetings; is that correct?

A. That's correct.

Q. And you had team meetings in person, team meetings over Skype, and team meetings by phone, correct?

A. That's accurate.

Q. They gave you an office at the CIA, or a room to work in?

A. I worked in a lab.

Q. You worked in their lab, right?

A. Yes.

Q. And when you worked in their lab, did they give you full access to what is a full image of the FS01 server?

A. Yes.

Q. And they gave you, did they not, access to the full image of the Atlassian server, correct?

A. That's correct.

Q. They gave you full access, did they not, to Mr. Schulte's workstation, correct?

A. Correct.

Q. You reviewed all of these -- I don't know, devices let's just call it. It's not precise, but you reviewed all of these devices and wrote up your reports on each one of them, correct?

A. I didn't specifically write a report for each one, but I did review all of the devices, yes.

Q. Okay. And you e-mailed each other about what you called were your sync-up efforts, correct?

A. To some extent, yes.

Q. You sent a lot of e-mails saying re sync-up effort.

What is that; what is a sync-up effort?

A. I don't recall writing an e-mail with that title.

Q. Okay. Do you know what a sync-up effort is when you would write it in your e-mail?

A. I don't know specifically what a sync-up effort is. I can tell you that we had sync meetings together.

Q. Okay. Tell us about these sync meetings.

A. Sure.

Q. How many times did you have them in a month?

A. It was more frequent toward the beginning of the case. I think they started daily, may have moved to weekly, and then eventually just scheduled individually.

(Continued on next page)

BY MS. SHROFF:

Q. Right. And then they peaked again, correct?

A. I believe so.

Q. Right. When you were preparing all these slides there, it picked up and peaked again, right?

A. Oh, more recently, yes.

Q. Now, in preparation for your testimony, the CIA set you up with the Atlassian Confluence server, correct?

A. Correct.

Q. And then you and FBI personnel together reviewed it, correct?

A. That's correct.

Q. And each time you reviewed it, you had a theory of prosecution in mind, correct?

A. Uh, I was aware, yes.

Q. What do you mean you were aware?

A. Uh --

Q. What does that mean?

A. I'm just saying that I was aware that the case was being criminally prosecuted.

Q. Well, you were aware of more than that, sir, right?

A. Yes.

Q. I mean, they had a theory of prosecution that they shared with you; you weren't kept in the dark. You're their expert, right?

A. Yes, but I didn't meet the attorneys here, I think, for a while in this case.

Q. Oh, yeah, yeah. There were many of them. All of them -- don't worry.

My question is whoever it is that told you, they told you what their theory of prosecution was, correct?

A. I believe so.

Q. Right. They didn't say to you: Hey, we don't know who did it. They came to you and said, We think Josh Schulte did it and this is how we're going to prove it, and you're going to work with us. Correct?

A. That's an unfair characterization of what happened.

Q. OK. Unfair or not, that's basically what happened, right?

A. I disagree.

Q. OK. Well, tell me how you disagree. Did they randomly, open-endedly tell you go find out who did it? No, right?

A. Yes, actually.

Q. Really?

A. Yes.

Q. OK. So tell us who else you looked at.

A. So, like I mentioned earlier, when I initially showed up, it was from an incident-response perspective, so --

Q. Could you answer my question?

A. Yes, ma'am.

MR. LAROCHE: He is answering the question.

THE COURT: Yes.

Q. Could you tell me --

THE COURT: Could we have the last question read back, please.

(Record read)

MS. SHROFF: No. Who else you looked at.

MR. LAROCHE: And he's answering it.

THE COURT: Tell us who else you looked at.

THE WITNESS: I remember the question. It's fine.

So, when I initially showed up, it was from an incident-response perspective, so we were looking at the every, the entire network in its entirety --

BY MS. SHROFF:

Q. Sir, I asked you which person you looked at as a suspect other than Mr. Schulte. That's my question.

A. I think suspect's a -- we looked at all of the other administrators; other -- all the other user workstations on DevLAN. We looked --

Q. That's not what I asked you, sir. I'm sure you looked at every workstation.

My question is did the government not tell you that they were prosecuting one person, and that was Mr. Schulte? Isn't that what they told you?

A. I think that's an unfair characterization of how the process worked.

Q. Sir, whether it's fair or unfair, could you answer my question?

A. Yes.

Q. OK. Did they tell you they were prosecuting Mr. Schulte?

A. I learned at a point he was being prosecuted, yes.

Q. Right. And they identified him as the suspect, correct?

A. Correct.

Q. And the CIA identified him as the suspect, correct?

A. Correct.

Q. They did not tell you: We don't know who the suspect is, take a wild guess or go investigate, correct?

A. Not in those specific terms.

Q. In fact, in no terms did they ever tell you that, correct?

A. I disagree.

Q. You disagree? Tell me one other person's name that you investigated as a possible suspect. Not a network, not a workstation, an individual that they told you to look at other than Josh Schulte.

A. Any of the other admins, for example.

Q. So they gave you a list of admins and they said all of these people are possible suspects and we might prosecute any one of them? Is that what they told you?

A. No, not in those specific words, but --

Q. In fact, in no words did they ever tell you that, correct?

A. I disagree.

Q. OK. So tell me one other name they told you.

A. I don't know the, like, the list of all the admin names offhand, but there's --

Q. You're the one who is telling me my characterization is unfair, correct? So tell me, which other -- let me make it easy for you.

Did they ever tell you an employee who took a screenshot of what happened on April 20 and said, Hey, he's possible suspect; take a look?

A. That's a fair characterization.

Q. They didn't tell you that, right?

A. That's a -- I would say that's a fair, like, characterization of the investigation.

Q. Put aside fair or not. Just answer my question, sir.

A. Yes.

Q. Other than Mr. Schulte -- I'll try it another way.

Are you aware that the government had a theory that this information was stolen in March rather than April of 2017 -- I mean '16?

A. Yes.

Q. You're aware of that, right?

A. Yes.

Q. First, they had this whole theory that the information had to have been stolen in March of 2016, correct?

A. I don't remember the specific details.

Q. You don't remember the details?

A. No.

Q. Do you remember if they filled out any search warrants with that date?

A. I don't remember.

Q. Did they tell you that they filled out search warrants with that date?

A. I don't remember to that specific date, no. I don't believe I've reviewed the contents of the search warrants, like, in their entirety.

Q. I'm not asking you if you reviewed the contents of any search warrants. I'm asking you very simple questions here, sir.

Did the FBI ever tell you that they were sure -- they were so sure that they signed an affidavit and gave it to a sitting federal judge -- that this information had been stolen not during a reversion on April 20 but in March of 2016? Did they tell you that?

A. I don't remember.

Q. You don't remember?

A. No.

Q. Your testimony here is that from the moment you started on this case, the only date you focused on as the date the information was taken is April 20; is that your testimony?

A. No. That's incorrect.

Q. OK. So you didn't know about the March 2016 date, correct?

A. Correct.

Q. You didn't know about the search warrants, correct?

A. No.

Q. You didn't know how many search warrants the FBI filed with that date telling a judge that's the date it was stolen, correct?

A. No.

Q. So as the forensic investigator, you never, ever investigated that date, correct?

A. I don't believe so.

Q. They never told you: Hey, eliminate this date for us. You're the forensic analyst working independently. Correct?

A. I don't remember.

Q. You'd remember that now, wouldn't you? I mean, you're an expert.

A. Yes.

Q. OK. So is it possible that you don't remember because they never told you that they had the wrong date?

A. Yes.

Q. OK. How many months have you worked with Mr. Laroche here who did your direct?

A. Maybe the last six months or so. Maybe --

Q. Six months?

A. Maybe not quite that long. Like, directly, yeah. It's been kind of on and off.

Q. For six months you've been talking to Mr. Laroche, right?

A. I believe that's accurate.

Q. Right. And let's just stay focused -- we're in February now. Let's just stick with January of 2020. All told, how many hours did you spend with him?

A. In January?

Q. Right.

A. Uh, maybe 80. 80 hours, maybe.

Q. 80 hours?

A. Maybe less than that.

Q. OK. How about the man next to him; Mr. Denton?

A. Significantly less. I mostly interacted with Mr. Laroche.

Q. And how about Mr. Kamaraju?

A. Same as Mr. Denton.

Q. And it's fair to say that your primary contact was with Mr. Laroche and the other two stepped in and stepped out? Correct?

A. That's accurate.

Q. And your testimony is, sitting here today, Mr. Laroche never told you about any possible March 2016 date as the date that table had identified as a date of theft, correct?

A. No. No. That's incorrect.

Q. That is correct, right?

A. It's incorrect. So, I do remember now the date, but just not from the beginning of the investigation when you were referring to earlier. I've heard about it, especially recently, as we were preparing for trial.

Q. So you didn't hear about it through all of your investigation, but then you only heard about it when you were preparing for trial; that's your testimony?

A. That's what I remember.

Q. That's what you remember?

A. Yes, ma'am.

Q. Hey, did you tell them --

A. Did I tell them?

Q. -- should I go back and check the March 16 date? Did you tell them that?

A. No.

Q. OK. Now, in terms of your investigation -- let's just stick to your investigation -- right, you looked at various networks? Correct?

A. Yes, ma'am.

Q. You looked at various workstations, correct?

A. Correct.

Q. You looked at various software programs, correct?

A. Correct.

Q. And you looked at various databases, correct?

A. Correct.

Q. Could you tell me, what is a TOU-DNS database?

A. OK. Could you say that again a little slower, please?

Q. Sure. Do you know what a TOU-DNS database is?

A. I'm not, like, familiar with the T-O-U, but a DNS database would mean to me, like, domain name service, so essentially a database of host names, mapping to IP addresses.

Q. And if you looked at it and you sent an email back to the prosecution team here that said that your search did not return any useful results, what would be a useful result for you?

A. It would really depend on the situation.

Q. OK. Now, you also testified, did you not, that you were told about what the CIA's system was, but you were kind of familiar with it because you're an expert in this field? Correct?

A. In networks, yes.

Q. Yes.

And when you were given access to DevLAN, were you given a mirror image to work with at the CIA?

A. Could you be more specific?

Q. No.

A. So, by mirror image, what does that encompass?

Q. Let me make it easy for you. You tell me what you were given.

A. Sure. We were given images of all of the DevLAN machines -- computers, servers -- that were available at the time that we showed up to analyze.

Q. All of them, correct?

A. Yes.

Q. Now, you testified that you were also given access to the Atlassian server, right?

A. Uh, yes.

Q. OK. And do you recall that you worked with an FBI agent named Berger to restore the Atlassian server? Do you remember that?

A. Yes. I don't remember which server specifically you're referring to.

Q. OK.

A. But we did restore a server together.

Q. And is it fair to say that the CIA gave you access all throughout the three years you worked with them on this case? Correct?

A. Yes.

Q. And working on this case itself, is it fair to say, because I know you like that phrase, is a good professional opportunity for you?

A. Yes.

Q. Right. Furthers your career, correct?

A. Yes, it does.

Q. It allows you to get more work from the FBI, correct?

A. Uh, I disagree with that.

Q. You do?

A. Yeah. I don't do our contracting, so I don't choose what work we get or don't get.

Q. No, no. I'm not asking you what work you choose. I'm just asking you if it was a step toward getting more work from the FBI for your company?

A. Uh, yes.

Q. And is it fair to say, sir, that you have attended as a spectator, sitting in that block over there, the entire trial up until this point? Correct?

A. That's correct.

Q. You've sat through all of the testimony, is that correct?

A. That's correct.

Q. You've heard every single piece of testimony that came into this trial through the people who work or worked at the CIA, correct?

A. That's correct.

Q. And these are the people you come to court with every day, yes?

A. Some of them, yes.

Q. You sit with them in that block, correct?

A. Correct.

Q. You have lunch with them, correct?

A. Correct.

Q. You talk with them on the break, correct?

A. Yes.

Q. In fact, on the break, Special Agent Evanchec gave you a nice pat on the back after had left, correct?

A. Yes.

Q. And with them, you know exactly what testimony has come in about Mr. Schulte, correct?

A. Correct.

Q. About the Atlassian servers, correct?

A. Correct.

Q. About DevLAN, correct?

A. Correct.

Q. About April 16 snapshot, correct?

A. Correct.

Q. April 20 snapshot, correct?

A. I don't believe there's a 20th snapshot. Aside from the defendant's snapshot, yes.

Q. It's not the defendant's snapshot. It's an April 20 snapshot that you think is the defendant's snapshot, correct?

A. Correct.

Q. You weren't there on April 20, correct?

A. Correct.

Q. Right. You know all of those facts, correct?

A. Yes.

Q. Right. And knowing all of those facts, you made this slide that's 105, correct?

A. Correct.

Q. Right. And the slide that is cut off to not show the jury that the San Disk was disconnected at 5:22 p.m., your testimony was that that slide presentation was inadvertent?

A. My --

Q. I just want a yes or no.

A. Yes.

Q. OK. Let me move on to a different topic, if I may.

Sitting here today, you are in agreement with me, are you not, sir, that it is the government's theory that Mr. Schulte created a snapshot of Confluence on April 20 at 5:29 p.m.? Correct?

A. I believe that's accurate.

Q. Well, you tell me. You're the expert.

A. Well, I'd want to see a time stamp to confirm that that's accurate.

Q. Take your time. Go ahead. Check the time stamp.

A. I don't have the snapshot. It was reverted 5:35, so before that it's accurate.

Q. Do you have your slide deck there, or should I give you mine?

A. No. It's up.

That's correct, 5:29 p.m.

Q. And according to them, and you, Mr. Schulte created that April 20 snapshot and called it backup, correct?

MS. SHROFF: If you could pull up slide 107.

Oh, there it is. Sorry about that. He's ahead of me.

Q. Slide 107 shows you that, correct?

A. Incorrect.

Q. Oh. OK. It doesn't show you the name there, backup?

A. Well, it's not backup. It's BKUP.

Q. My bad. It shows you a slide that is the backup. It's called B-K-U up. Is that how you want me to refer to it, or should I call it BKUP; which one?

A. BKUP's fine.

Q. OK. So on April 20, according to you, Mr. Schulte took an April 20 snapshot and called it B-K-U up, correct?

A. Correct.

Q. And according to all of you, Mr. Schulte then reverted, did he not, to an earlier state, and that earlier state is BK-4-16-16? Correct?

A. That's correct.

Q. I just want to get the timings down here.

And according to you and the government, this is around 5:35 p.m. on April 20?

A. That's correct.

Q. OK. And then, according to all of you, at about 6:51 p.m., Mr. Schulte's workstation was used to revert back to the April 20 snapshot of Confluence, correct?

A. That's correct.

Q. And that is the snapshot called BKUP, correct?

A. Correct.

Q. OK. Now, let's see if we can focus your testimony to the time period on April 20 between 5:35 p.m. and 6:51 p.m. OK?

A. OK.

Q. And just to make it easy on you, me and everyone else, let's just call that the reversion period. OK?

A. OK.

Q. And just to be sure you and I understand reversion the same way, that is roughly the time when Mr. Schulte, according to you, went to the April 16 snapshot and then returned back to the 4/20 snapshot?

A. That's correct.

Q. OK?

A. That is the time, yes.

Q. Now, you and I agree, right, that Mr. Schulte did not create the April 16 snapshot? Right?

A. That's correct.

Q. The April 16 snapshot was created by a team of CIA employees who came in to the CIA on that Saturday, April 16, and created the snapshot, correct?

A. Correct.

Q. That was Jeremy Weber, is that right?

A. Yes.

Q. Mr. Tim, right?

A. Uh-huh.

Q. And David?

A. Correct.

Q. By the way, have you met Mr. Weber?

A. I have, yes.

Q. And have you met Mr. Tim?

A. I don't believe I've met Tim.

Q. And how about Mr. Dave?

A. I have met Dave.

Q. And to stay focused, and back to this issue, this reversion is the time that the government claims that Mr. Schulte accessed the Confluence backup file, correct?

A. That's correct.

Q. And this Confluence backup file was on the Altabackup, correct?

A. Correct.

Q. And according to you and the government, shortly afterward, during this reversion period, the theory is that he also accessed the Stash backup file, correct?

A. That would be correct.

Q. And both of you -- or all of you claim that he did this, right, also by accessing the Altabackup? Right?

A. Correct.

Q. So in essence, all of you agree that this period of time is basically your crime-scene time, correct; this is the time of the crime?

A. Correct.

Q. This is when, according to all of you, he's stealing the data; this is the heist period -- you go to a bank, you heist it, heist period -- he's heisting it, correct?

A. Correct.

Q. And I'm assuming that you don't disagree with their theory. Correct?

A. Correct.

Q. Let me see if I can pull up for you Government Exhibit 1207-27 and Government Exhibit 1207-30. I apologize if I'm going slower than normal, but this is not my bailiwick. OK? So just bear with me.

A. No. You're fine.

Q. There are many columns here, and the government has shown you these two exhibits several times, is that correct?

A. That's correct.

Q. And you see that column that's titled "name"?

A. Yes.

Q. OK. Just tell me, what exactly do these names mean to you?

A. So, this is the name of the backup file. If -- when we looked at the script, this name is generated based on that. So there's the time the file was made. There's the name of the service and then whether it's the database or the home folder.

Q. OK. So it's fair to say that you don't know who gave these files these names, correct? They're just names to you; right?

A. No. They were named by the backup script.

Q. Right. There's not a human being who gave them the names, correct?

A. Oh, correct.

Q. OK. That's what I meant.

Now, next to this column is a column that reads "date modified," right?

A. That's correct.

Q. And there's a date modified on 1207-27 and there's a date modified on 1207-30, correct?

A. Yes.

Q. And then next to that is a file type for each one of these things, right?

A. Correct.

Q. There's a SQL file and a win -- I know you're particular, so is it R-A-R or RAR? How do you say that?

A. WinRAR archive.

Q. SO those are the TWO types of files on Government Exhibits 1207-27 and 1207-30, correct?

A. That's correct.

Q. And then the column after that tells you the date these files were accessed, right?

A. That's incorrect.

Q. Oh, I skipped size. It tells you the size of the files, correct?

A. Yes.

Q. My bad. Sorry.

A. That's all right.

Q. And then after that it tells you the date on which these files were accessed, right?

A. Correct.

Q. And the last column tells you that these are the dates these files were created, right?

A. That's correct.

Q. OK. Now, I'm just going to see if I can simplify this to understand it a little better. Just imagine these two documents are simple Word documents, like a list that I made at home. OK?

A. Uh-huh.

Q. I don't know, a list of food items I wanted to buy or shoes I wanted to buy, or whatever it is, books, whatever.

A. Uh-huh.

Q. I make a list. OK. I put the Word document and I save it. I save it to documents on my computer. Correct?

A. Correct.

Q. And the date created is the date that I first made that list, right?

A. For the, like, date-created column?

Q. Yeah.

A. Uh, yes.

Q. Right. That's the date I first decided to make my shopping list, correct?

A. Correct.

Q. Right. OK. And then the date modified is a day or date that I either read my list or make a change to my list, correct?

A. That's correct.

Q. That's the date modified, correct?

A. Uh -- reading it may not update the modified time, but changing the content of it will.

Q. OK. So you don't think that if I read it it will change the time, but if I change it it will change the time; that's your testimony?

A. For the modified column?

Q. Yes.

A. It depends.

Q. OK. So you don't know?

A. No. It depends.

Q. OK. And then the date accessed would be the very last time I read or saved that document, correct?

A. That's accurate.

Q. OK. So the very last time that I go into the list and check what items are on my list, that's the date accessed that will save, correct?

A. To some extent, yes.

Q. What do you mean some extent?

A. Well, so, the access time could be, like, the time it was created if you were, like, putting the file on the server.

Q. I don't have a server. This is a simple Word document that I have. The date I access it, if I open it and I re-save it, it saves with a new date as being accessed, correct?

A. Correct.

Q. And neither in your chart or my hypothetical is there a column that says date copied, correct?

A. Correct.

Q. There is no column that says date copied on 1207-27, correct?

A. Correct.

Q. And there is no date copied on 1207-30, correct?

A. Correct.

Q. And all that this tells you is that someone -- you've identified for yourself who, but someone opened or read or accessed that column, correct?

A. Yes.

Q. OK. So the accessed time alone does not tell you at all if anyone ever copied that file, correct?

A. Uh, that's not entirely accurate.

Q. Well, OK. Tell me how it tells you that somebody copied it.

A. Well, the access --

Q. Just listen to my question, please. OK?

A. Uh-huh.

Q. My question is, looking at the two exhibits --

A. Uh-huh.

Q. -- putting aside the theory you all have floated for yourselves --

A. Uh-huh.

Q. -- just looking at the column, looking at the log --

A. Uh-huh.

Q. -- does it tell you whether or not it was copied?

A. It could.

Q. Does it, sir? If I showed this to you, ran into you on a subway and I say Mr. Expert, can you tell me if any of these files were copied, you couldn't tell me, right?

A. That's inaccurate.

Q. Looking at these logs you can tell me if it's copied? Tell me how.

A. I can tell you that it could have been copied. There's a difference between can't say that it was copied at all or could have been copied. The access time can be updated from file copying.

Q. Really?

A. Yes.

Q. You think there's a difference in telling me it could have been done, maybe it was done, perhaps it was done, and it was done, right?

A. Or it was not done.

Q. Those are very different things, right?

A. Correct.

Q. Or not done, correct?

A. Correct.

Q. So you can't tell me it was done, correct?

A. Correct.

Q. You can't tell me it wasn't done, correct?

A. That's correct.

Q. Right. You can't tell. All you can tell is what that document showed you. It showed you -- let's just randomly pick one -- Confluence blah, blah, blah-625 TGZ. All you can tell me is the date accessed that shows on the document, right?

A. That is correct.

Q. And if I could go back to the first two, 1203-54, if you look at the timings here and you look at the timing of the disconnected San Disk, the disconnected San Disk is at 5:22?

A. Yes, that is correct.

MS. SHROFF: OK. Let's go back to the other one, to the access log.

Q. Do you see anything there before the disconnect on 5:22?

A. Before?

Q. No, right?

A. No.

Q. OK. So the San Disk's already out?

A. That is correct.

Q. OK. So now your theory about it being copied --

MS. SHROFF: You know what? I'll withdraw that.

OK. You can take that one down.

Q. Now, let me ask you something. You testified about the ways that a computer can copy a file, right?

A. Uh, I believe so.

Q. OK. And as an expert, you would be able to agree with me that one way to copy a file is to use what is called a copy command, correct?

A. That is -- that is correct.

Q. Right. And just for those of us who are not all that computer savvy, a command is just telling the computer what you want it to do, right?

A. Yes, that's correct.

Q. And the command is called an SCP command?

A. That's a different type of command.

Q. OK. An SCP command is a command that's run on Linux, correct?

A. Yes, it is.

Q. And we've already established for all of us that Linux is just like Word, just some people use Linux, right?

A. Yes.

Q. OK. So the SCP command is a command that allows you to copy a file on Linux, right?

A. It's a little more complicated than that, but yes.

Q. Isn't it a command that lets you copy a file from Linux?

A. Yes.

Q. OK. And you looked when you were doing your forensic analysis -- for the last three years, right? You looked to see if there was any copy command, right?

A. On the server, yes.

Q. Everywhere.

A. Yes.

Q. You looked, right?

A. Yes.

Q. OK. I mean, you really looked, right?

A. Yes.

Q. OK. Did you find a copy command?

A. Uh, I'm sure there were copy commands used all over the network.

Q. Come on. Sir, I'm asking you if you found any copy command that would allow you to sit here and testify that you have any forensic indication of a file actually being sent a command to copy. You know that's my question, and if it wasn't clear, it's clear now. Did you find such a command?

A. No, not in respect to the Altabackup, which I think you're referring --

Q. We're only talking about the Altabackups, right?

A. Well --

Q. Did you find --

A. I'm sorry.

Q. Did you find any --

(Counsel conferred)

Q. Mr. Zas is kind enough to ask me to remind you that we're still talking of that time period where I told you that we were talking about that reversion period. Right?

A. Yes.

Q. OK.

A. The answer to your question's no.

Q. You found no copy command, right?

A. I believe so, yes. That's correct.

Q. No, no. "I believe so" is a hard answer for me.

A. I'm sorry.

Q. Yes or no. You found none, right?

A. Yes.

Q. Yes, you found none?

A. Correct.

Q. They asked you to look to see if there was a copy command during the reversion period, correct?

A. Correct.

Q. You wanted to find a copy command during the reversion period, correct?

A. Yes.

Q. And you did not find one, correct?

A. That's correct.

Q. How long, according to you, was the reversion period?

A. Uh, it was over an hour. Maybe like an hour and 20 minutes, I think.

Q. And for that hour and 20 minutes, the time before and the time after, there's no forensic indication of any copy command, correct?

A. Do you mean during?

Q. Just the reversion period.

A. OK. No.

MS. SHROFF: Your Honor, would this be a good time for our lunch break?

THE COURT: Yes.

MS. SHROFF: Thank you.

THE COURT: We'll take our luncheon break now and resume at 1:30.

(Continued on next page)

(Jury not present)

THE COURT: You're on cross-examination now, so don't be talking to anybody on the government's trial team.

THE WITNESS: Yes, sir.

THE COURT: See you at 1:30.

(Luncheon recess)

AFTERNOON SESSION

1:30 p.m.

(In open court; jury not present)

MR. ZAS: Your Honor, just one quick matter. You remember yesterday we talked about a possible instruction on experts?

THE COURT: Yes.

MR. ZAS: At this point in the case rather than at the end?

THE COURT: Yes.

MR. ZAS: I conferred with the government. I think we're in agreement that a good time might be at the completion of this witness's entire testimony.

THE COURT: I'm reconsidering whether I've got to issue an instruction at all, and save it for when I give the instructions at the end of the case.

Bring in the jury.

MR. ZAS: We prefer it now just because --

THE COURT: Bring in the jury.

(Continued on next page)

(Jury present)

THE COURT: All right, Ms. Shroff.

MS. SHROFF: Thank you, your Honor.

BY MS. SHROFF:

Q. Now, sir, before we broke for lunch, you testified, did you not, that you found no evidence of a copy command on Mr. Schulte's desk top for the reversion period. Correct?

A. That's correct.

Q. Is it also true, and forensically accurate, that during the reversion period you found no forensic evidence of any storage device connected or being connected to Mr. Schulte's workstation, correct?

A. That's correct.

Q. And when we're talking about a storage device, we mean something that would allow a person to exfiltrate data from one place to another; is that correct?

A. Correct.

Q. To exfiltrate data, just so we're all clear, is to take data or information out of a network or a computer, correct?

A. That's correct.

Q. So to exfiltrate data, you would actually need removable media, correct?

A. Not necessarily.

Q. If it was an air gapped network, you would need removable media, right?

A. Yes.

Q. Okay. Just want to be crystal clear. Between the time period of 5:35 p.m. and 6:51 p.m., sir, you did not see any evidence whatsoever of any removable media connected to Mr. Schulte's workstation, correct?

A. Correct; yes.

Q. Let me ask you a quick question. When you were looking at the April 20 dates and the logs, correct?

A. Correct.

Q. You looked and you focused on times and dates created and times and dates accessed, correct?

A. I believe so.

Q. Right. And then you looked at all the timings on a file, correct?

A. Yes.

Q. And by the way, do you know what a touch command is?

A. Yes, I do.

Q. What's a touch command?

A. The touch command is a command in Linux that you can use to create new files. You can also use it to edit time stamps for files as well.

Q. When you say "edit time stamps," you mean change time stamps, correct?

A. Yeah, I believe you can change them, modify and access times, but not the see time.

Q. But when you say modify, change -- what was the other word you used?

A. I think that was it.

Q. Okay. So that means you can use a touch command, change the time that a file shows at the time it was accessed, right?

A. It can be used for that, yes.

Q. Right. By the way, you would agree with me, would you not, that the CIA has, at least in the EDG group, at least 200 developer, correct?

A. That's accurate.

Q. Right?

A. Yes.

Q. Talented people, correct?

A. Yes.

Q. Smart people, correct?

A. Yes.

Q. All 200 know what a touch command is, right?

A. I don't know about that.

Q. Really? You have doubts that somebody at the CIA knows what a touch command is? Okay.

Now, sir, you did not know Mr. Schulte on April 20, correct?

A. No, I did not.

Q. And you were not at the CIA on April 20, correct?

A. No.

Q. 2016, 2017, at all, correct?

A. No.

Q. Never saw him walk out with a removable device, correct?

A. No, I did not.

Q. Never saw him with a thumb drive walking out of the CIA, correct?

A. No.

Q. You have no idea what the physical security was at the CIA on April 20, 2016, until November 10, 2016, correct?

A. That's incorrect.

Q. 2016? You were there in April of 2016?

A. I was not, no.

Q. So you have no personal knowledge of what it was like, correct?

A. From firsthand experience, no.

Q. Right. That's personal knowledge.

A. Oh.

Q. Do you have personal knowledge, sir?

A. No.

Q. All you know is what somebody told you, correct?

A. That's correct.

Q. Everything somebody told you either came from the FBI, correct?

A. Correct.

Q. Or the CIA, correct?

A. That's correct.

Q. Okay. Now, you've talked a lot about all the work you did at the CIA, correct?

A. Correct.

Q. And there are many removable media that people at the CIA use, correct?

A. Yes, that's correct.

Q. They use thumb drives?

A. Correct.

Q. Over and over again, right?

A. Yes.

Q. Right. You use the thumb drive to create malware, correct?

A. In some cases, yes.

Q. Right. You test it out, correct?

A. Correct.

Q. And then if there is a problem, you start over, correct?

A. Yes.

Q. Okay. Every time you create malware, you don't throw out the thumb drive, right, if it doesn't work?

A. I don't know. I would assume not.

Q. You assume not?

A. Well, I didn't develop the tools myself.

Q. Oh, God no, but you spent hours and hours talking to these people about developing tools, correct?

A. Yes.

Q. Is it fair to say, sir, that one of the ways to erase a thumb drive is what we call or you called zeroing a thumb drive, correct?

A. I didn't use that term specifically, but yes.

Q. Zeroing a thumb drive means you delete every single file from the thumb drive, right?

A. It's more in depth than that, but yes.

Q. It's not really more in depth than that. It just means there is zero file strokes on a disc. That's it, right?

A. Yes.

Q. I think all the tech people -- never mind. I'll withdraw that.

It is a fancy way of saying that you want to make sure that when you use that thumb drive again, there's nothing on it, right?

A. Correct.

Q. Okay. And let me ask you this. How many times in a day would a developer zero a thumb drive?

A. I have no idea.

Q. Okay. That's because you're not a developer?

A. Not on that network, no.

Q. But -- on any network.

A. I do software development.

Q. Right, and you would zero a thumb drive before you reuse it, right? It's just common practice, correct?

A. It depends.

Q. Okay. You would reuse a thumb drive in starting a brand new project without zeroing it?

A. Yes.

Q. Why?

A. Like I said, I don't develop USB tools.

Q. Okay. If you were developing a USB tool, you'd zero it?

A. It really depends.

Q. Say it again?

A. It depends.

Q. Okay. When you examined -- did you by any chance actually physically examine any thumb drives that Mr. Schulte used?

A. I had images of those thumb drives. I've seen pictures for them, but I had forensic images of them.

Q. You had a full forensic image, correct?

A. That's correct.

Q. How many thumb drives did you have a full forensic image of?

A. A lot.

Q. A lot. How many is a lot?

A. Over the network, there were -- dozens.

Q. Right, and you had physical -- I mean, you had access to every one of those mirror images, correct?

A. Yes.

Q. In fact, you had access to the mirror images of almost every network and every computer that you needed from the CIA, correct?

A. Yes.

Q. And that very much informed your expert opinion here, correct?

A. Correct.

Q. By the time you examined the -- let me call them the Schulte thumb drives, okay?

A. Hmm-hmm.

Q. How many months had he been gone from the CIA?

A. Who?

Q. He had left the CIA by the time you examined them, correct?

A. Oh, the defendant?

Q. Yes.

A. Yes.

Q. I'm only talking about Mr. Schulte here.

A. Hmm-hmm.

Q. Okay. And by the way, where did you find the thumb drives in his desk drawer?

A. I don't remember where they were found. I didn't physically see them myself.

Q. You didn't see them yourself?

A. No.

Q. For all you know, he just left them in his desk and left, right?

A. Yes.

Q. You just don't know?

A. Yeah, I don't know.

Q. Let's see if we can move on to Government Exhibit 1203-18. Let me know when you're ready.

A. I'm ready.

Q. Okay. So you see that thing that says root@OSB colon squiggly thingy closed brackets DF-H?

A. Yes.

Q. Okay. And when you were testifying, you testified about that highlighted portion, correct, on direct?

A. I don't believe we covered the DF command. But, oh, I'm sorry.

Q. You didn't cover it?

A. The black highlighted portion.

Q. You covered the portion that I'm not covering.

A. That's correct.

Q. I'm covering the portion you didn't cover.

A. Sure.

Q. Okay. And this, this command, right, would you agree with me that it is a simple command used to see how much disc space is free?

A. That's correct.

Q. Okay. And this is a very typical run-of-the-mill command, correct?

A. Correct.

Q. It is just a normal, regular run-of-the-mill command that any system administrator would take, right?

A. That's correct.

Q. And this is just to see if there is free disc space, right?

A. Correct.

Q. And it has absolutely zero to do with copying of any data, correct?

A. That's correct.

Q. Okay. You can take that down. Let's see if we can take a look, if we may, to Government Exhibit 1063. I must have the wrong number. Slide 70. This is it? Sorry.

You read that before, right?

A. Yes, I did.

Q. And you would agree, would you not, that a simple way to test out if your keys are or are not working is to just try to login somewhere, correct?

A. Yes, that's correct.

Q. Okay. One of the ways to make sure that your keys are or were revoked is to see if your keys are working again, correct?

A. Yes, that's correct.

Q. Okay. Would it be proper to try to use your keys as an adequate test for seeing whether or not your keys have been removed?

A. Yes, it would.

Q. Right. And that is in fact -- you can take that one down.

That is in fact what your friend Mr. Weber did on April 16, correct?

A. Yes.

Q. Okay. Is it fair to say that computers or workstations keep records of whatever removable device is inserted or removed into them?

A. Yes, that's true.

Q. And you, not you, only you, but a computer would keep track of when a foreign disc is inserted in, correct?

A. Correct.

Q. And when it's pulled out, correct?

A. Correct.

Q. Now, I am just going to go back for a minute -- I'm sorry to jump around -- to that Sandisk that you testified to.

A. Sure.

Q. Okay. Sitting here today, could you tell me, tell the jury, do you know the size of that Sandisk?

A. Yes, I do.

Q. What is it?

A. I believe it's 64 gigabytes.

Q. You believe?

A. Yes.

Q. Okay. Was there a 64 gigabyte in 2016?

A. Yes.

Q. How much data do you think you could load on to that, if in fact it was not disconnected, which it was, and didn't have a write block?

A. A little bit less than 64 gigabytes.

Q. And 64 gigabytes is, what, a quarter of what the government is alleging was stolen, correct?

A. That's correct.

Q. It's not even a quarter, it's less than a quarter, right?

A. That's accurate.

Q. Okay. No way it would have fit on that little thumb drive, right?

A. No.

Q. By the way, do you have any knowledge of how a tool gets compromised?

A. By a tool, do you mean like a tool from EDG?

Q. Yeah.

A. Like, academically, but not like first hand.

Q. You don't know, right?

A. No.

Q. You don't know how many tools in the WikiLeaks disclosure were or were not compromised, correct?

A. That's correct.

Q. Right. And in fact, you don't know if anyone else knew which of the CIA's tools were compromised, correct? You certainly don't know, right?

A. That's accurate, yes.

Q. Now, you testified and I think Mr. Laroche covered this with you, this concept of unallocated space, right?

A. Yes.

Q. Unallocated space is just basically space that someone's not using, correct?

A. That's a fair statement, yes.

Q. Right? That's all it is?

A. Hmm-hmm.

Q. Right. So on any given network, there is unallocated space, right?

A. Yes.

Q. Any given workstation, there is unallocated space, correct?

A. Correct.

Q. In fact, if one of us went home tomorrow and decided to find out if we had unallocated space on our computers, we would be able to find that too, correct?

A. Correct.

Q. It is a person's job, if they are maintaining a system, to make sure that there is ample unallocated space, correct?

A. If you wanted free space to store your files, yes.

Q. Well, don't you need free space to develop work?

A. Yes.

Q. You need free space to do work, correct?

A. Correct.

Q. And we're all in the business of doing work, right?

A. Yes.

Q. You need unallocated space, right?

A. Yes.

MS. SHROFF: I have nothing further, your Honor. Thank you.

THE COURT: Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

REDIRECT EXAMINATION

BY MR. LAROCHE:

Q. Mr. Leedom, you were asked a number of questions by Ms. Shroff related to how this investigation was conducted.

A. Yeah, that's correct.

Q. Let me just ask you, was it a foregone conclusion that Mr. Schulte was going to be charged in this case?

A. No. No, it wasn't.

Q. Why don't we talk through what happened at the beginning of this investigation.

A. Sure.

Q. Now, you said that you were deployed to CCI; is that correct?

A. That's correct.

Q. Can you tell us, when you first got there, what were some of the things you did at CCI?

A. So, we first arrived on site and we were just kind of trying to figure out how to -- we had a lot of people, so we had to find a way to get them to work together and start looking at the data. The FBI has a group that actually does the physical, like, imaging of computers. So they came and had started that process before I got there. So, essentially, like, taking the physical hard drives and turning it into an image that analysts can look at. So, they were still finishing up that process, and we were trying to figure out a way to tackle the large volume of data.

And myself, specifically, I was looking at it from an incident response perspective. So, I didn't know at the time, like, who may or may not have done it or even honestly what had happened. So, my main concern was to look at the machines we were given, and just see if there were any kinds of like evidence of intrusion activity, or any kinds of like root kits on the system, things like that. That was kind of how the first few weeks went for me.

Q. What type of intrusion activity were you looking for?

A. Specifically knowing it is the CIA, and like, obviously, like, a nation state type activity.

Q. Is Mr. Schulte a nation state?

A. No, he's not.

Q. Why were you looking for nation state activity?

A. Because we, like I said, we didn't really know, at least I wasn't like told initially, who or what they thought had happened. So I was just looking at it kind from an outsider's perspective what could have happened to the network.

Q. I think a few times you started to say reviewing the administrators and you were cut off?

A. That's correct.

Q. Can you say what you were trying to say about the review of the administrators' computers?

A. Shortly after going into the investigation, when we started to realize, like, what had been taken, and that it related to some of what could have been the backup files or the stuff on the ESXi server, we knew that those were kind of, like, since they were servers, they were run by the administrators. So the, you know, first people on the list of people to see who had access to it, of course, were these administrators.

So we tracked these people down. Several of them have testified already. And those were the first machines that got pulled to get looked at to start looking to see what happened.

Q. Why were you looking at the administrators' computers?

A. A normal user on the network wouldn't have the access required to, you know, get in some of these different services.

Q. Let's talk about the regular users. Did the FBI look at the regular users' computers as part of this investigation?

A. Yes.

Q. Was that beyond Mr. Schulte?

A. Oh, yes.

Q. How far beyond Mr. Schulte?

A. A lot. There were, there were a lot of machines, it was -- it was a very technically challenging problem to analyze and review all of those machines thoroughly.

Q. Why?

A. When you have -- I don't remember the exact numbers, but it was certainly -- like, we had over thousands and thousands of terabytes worth of data from this network. I mean, imagine, you know, you have hundreds of workstations, some users had more than one workstation, and you have to look at all to try and figure out, you know, what's useful, what's not.

Q. On those other machines, let's just focus on the administrators. How many of the other administrators deleted log files as part of their work at CCI?

A. None.

Q. You were asked a number of questions about this USB device.

A. Yes.

Q. If I recall your presentation, that was activities that happened before 5:30 p.m., is that correct?

A. That's correct.

Q. Which slide of your presentation says that the data was stolen on that USB device?

A. There's no slide that says that.

Q. Why not?

A. Because I don't believe that's what happened.

Q. Why is that?

A. I did a lot of USB forensics on the machine, and also reviewed the logs that we showed, and you know, and as Ms. Shroff pointed out, the drive itself is only 64 gigabytes. It would not have held all the data.

Q. I think Ms. Shroff started to ask you a question that she withdrew, and I think I knew the question she was going to ask, and I am going to ask it to you.

MS. SHROFF: Objection. How would he know?

THE COURT: He is a good guesser.

MS. SHROFF: I think you should sustain that objection.

MR. LAROCHE: I'll ask the question.

Q. Does the fact that that USB device was removed before the reversion change your opinion that the defendant copied those backup files on April 20, 2016?

A. No, it does not.

Q. Why not?

A. Because of all of the other surrounding evidence. We have the logged deletions, we have the access on the server, and things like that. That's much more telling. There's many other ways you can steal files from the network.

Q. Now, you were asked a question about whether you consulted with the defense; do you remember that?

A. Yes.

Q. You initially said yes?

A. Yes.

Q. Did there come a time when you agreed to meet with the defendant's expert?

A. Yes.

Q. Do you see that individual in the courtroom today?

A. Yes, I do.

Q. Has he been here throughout the case?

A. Yes, he has.

Q. Who is that?

A. Mr. Bellovin.

Q. Why did you agree to meet with the defendant's expert in this case?

A. The discovery process was obviously difficult in the case. So, I went to speak with him just to kind of come to common ground and figure out what we had that defense had wanted, and what we could provide and what was available.

Q. Fair to say to try to assist him in this case; is that right?

MS. SHROFF: Objection.

THE COURT: Overruled.

Q. Fair to say you were trying to assist him in this case; isn't that correct?

A. That's correct.

Q. You were asked a number of questions about a copy command.

Isn't that right?

A. Yes.

Q. And whether you found a copy command on the system during the reversion; is that correct?

A. That's correct.

Q. You were also asked a number of questions about logs relating to storage devices. Correct?

A. Yes.

Q. And whether you found logs related to storage devices during the reversion?

A. Correct.

Q. Can you just summarize for us the different types of logs that the defendant deleted on April 20, 2016?

A. Yes. So, the defendant deleted from the server itself pretty much all the core system logs for the server. So it would have shown all the things Mr. Laroche mentioned, and, of course all, you know, basic system activities at the time. It's hard to say what is there because it's all gone. But, that's the type of basic activity.

And then from the virtual machine itself, the same types of logs, specifically, connections to the virtual machine, things like that.

Q. Would those types of logs have assisted you in identifying a copy command.

A. Yes, they would have.

Q. Would those types of logs have assisted you in identifying a storage device?

A. Correct, they would have, yes.

Q. The other thing that the defendant did on the 20th was, after the reversion was over, he reverted back to the bkup snapshot; is that correct?

A. That's correct.

Q. Did that have any effect on your ability to review his activities during that time?

A. It had a significant effect.

Q. What effect did it have?

A. All the activity during the one-hour reversion period was erased.

Q. You were also asked about an administrative command, DF-H command. Do you recall that?

A. I do.

Q. You were asked whether that was a regular command to be run by a system administrator?

A. Yes.

Q. What about all the log deletions on April 20, 2016. Is that a regular command to run by an administrator?

A. No. In fact, it's highly irregular.

Q. Why?

A. The only time as an administrator that you would delete logs is if they're too big to fit on the machine you're storing them on. And from the, I mean, the DF command we saw, even there, just there was plenty of space on the ESXi server, and those logs aren't very big. We saw even in comparison to the file size of the files in the Confluence virtual machine folder. That log folder is very tiny. So clearly, they weren't deleted because of a size issue. The only other reason you would delete log files is to hide activity.

MR. LAROCHE: No further questions.

MS. SHROFF: Your Honor, may I just ask one question?

THE COURT: Just this once.

RECROSS EXAMINATION

BY MS. SHROFF:

Q. Am I correct, Mr. Leedom, that there was not a single log file deleted from Mr. Schulte's workstation?

A. From his actual -- the host, the Windows workstation?

Q. Right. The workstation that he used, not a single file was deleted, correct?

A. I believe that's accurate.

MS. SHROFF: Thank you.

THE COURT: You are excused, Mr. Leedom.

(Witness excused)

THE COURT: Call your next witness.

MR. KAMARAJU: The government calls Michael, your Honor.

THE COURT: Okay.

MS. SHROFF: Thank you for the question, your Honor.

THE COURT: You're welcome.

THE DEPUTY CLERK: State your name for the record.

THE WITNESS: Michael.

(Witness sworn)

THE COURT: Please sit down. Okay, Mr. Kamaraju.

MR. KAMARAJU: Thank you, your Honor.

MICHAEL,

called as a witness by the Government,

having been duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. KAMARAJU:

Q. Good afternoon.

A. Hello.

Q. Sir, are you currently employed?

A. Yes.

Q. Where do you work?

A. The Central Intelligence Agency.

Q. What's the current status of your employment with the CIA?

A. I'm on paid administrative leave.

Q. Do you know why you're on paid administrative leave?

A. No.

Q. In 2016, were you also employed by the CIA?

A. Yes.

Q. Were you on administrative leave at that time?

A. I'm sorry, what was the question?

Q. Were you on administrative leave at that time?

A. No.

Q. At that time, in 2016, were you employed in any particular part of the CIA?

A. Yes.

Q. What part were you working in?

A. I was working inside of IOC's Engineering Development Group.

Q. Looking around the courtroom, do you see anyone who worked with you at EDG in 2016?

A. Yes. It is difficult, but yes.

Q. Can you describe where he's sitting?

A. He's in the back table, over there behind the computer monitor.

Q. Can you see an article of clothing he's wearing?

A. Black jacket.

MR. KAMARAJU: Your Honor, the government would ask that the record reflect that the witness has identified the defendant.

THE COURT: Yes.

MR. KAMARAJU: Thank you.

Q. Sir, you mentioned you were in EDG at the time, right?

A. Yes.

Q. When did you first meet the defendant?

A. In 2013.

Q. How did you come to meet him?

A. We worked together.

Q. Within EDG, were you in a particular branch at that time?

A. Yes.

Q. What branch was that?

A. The Operations Support Branch.

Q. How would you describe your relationship with the defendant?

A. We were friends. We were similar in age. Probably the only ones at that time that were similar to that age.

Q. Did you guys socialize?

A. Yeah, we would go to the gym after work, we would play video games together. We would hang out outside of work.

Q. Did you ever go to his house?

A. Yes.

Q. I think you testified you hung out outside of work; is that right?

A. Yes.

Q. Did you ever have arguments with him while at work?

A. Yes.

Q. Did those arguments ever result in any confrontations?

A. Yes.

Q. Did they ever turn physical?

A. Yes.

Q. Could you just describe generally what happened.

A. Sure. On that day, Josh hit me with a rubber band, I hit him back with a rubber band. This went back and forth until late at night. I hit him with a rubber band and then ran away before he could hit me back. He trashed my desk. I trashed his desk. And then I was backed up against Jeremy's desk and Josh was looking at me, kind of coming towards me. And something came over me and I just hit him.

Q. That kind of atmosphere, playing pranks on each other, was that common in OSB at the time?

A. Yes.

Q. Did there come a time when the defendant stopped working with you in OSB?

A. Yes.

Q. Was he still working within EDG?

A. Yes.

Q. Where in EDG was he working?

A. RDB.

Q. Did you still see the defendant after he moved to RDB?

A. Less so, but yes.

Q. What was the defendant's reaction to his move to RDB?

A. He was unhappy about it.

Q. Do you know why he was unhappy?

A. Because he felt like it was a punishment for reporting the issue with Amol.

Q. How do you know he felt unhappy about it?

A. He told me.

Q. Do you know a person named Jeremy Weber?

A. Yes.

Q. How did the defendant feel about Jeremy Weber after he moved to RDB?

A. He was unhappy with him.

Q. Generally speaking, what was the reason for that unhappiness?

A. He -- there was an argument over a project. Josh wanted to bring this project with him to the new branch, and Jeremy did not want him to bring that project.

Q. How did you know that the defendant was angry at Mr. Weber?

MS. SHROFF: Objection.

A. He told me.

THE COURT: Overruled.

A. He told me.

Q. Did you ever speak with Mr. Weber about the defendant's anger?

A. Yes.

Q. What did you talk about?

A. We didn't talk about his anger per se. But, I told Jeremy that he should remove all of Josh's admin accesses.

Q. Why did you ask Mr. Weber to do that?

A. I felt like Jeremy was kind of, like, setting him up. I knew that Josh was mad at Jeremy, and that he was putting him in a position where Josh had the ability or the access to change permissions on the project in question. And that he would do that because he didn't respect Jeremy's authority.

Q. What do you mean when you say he didn't respect Jeremy's authority?

A. Jeremy was kind of looked at like a senior developer, although he didn't have, like, an official title, he was just a developer like any of us. But he was -- he had been there longer than us, and he led some of our development teams.

Q. Did that bother the defendant?

A. Yeah, he didn't think it was fair that this person without an official title was getting to make calls about, you know, who should take a project and those types of things.

Q. I'd like to direct your attention to April 20, 2016. Were you working in OSB at that time?

A. Yes.

Q. And by that time, had the defendant been moved to RDB?

A. Yes.

Q. Generally speaking, how did you communicate with the defendant at work?

A. After the move?

Q. Sure. After the move.

A. Via instant messaging systems.

Q. Have you heard of something called Same Time?

A. Yes.

Q. What's Same Time?

A. Same Time is the instant messaging system we use on our high side system.

Q. When you say high side, just for all of us, does that mean the classified system?

A. Yes.

Q. Did you ever Same Time with the defendant?

A. Yes.

MR. KAMARAJU: Ms. Hurst, can we publish Government Exhibit 719 which is already in evidence.

Q. It should show up on your screen, sir.

A. I see it.

Q. All right. What are we looking at here?

A. This is a Same Time log between Josh and myself.

Q. What's the date of this exchange?

A. It is April 20, 2016.

Q. You see the first message there?

A. Yes.

Q. What time was that message sent?

A. 17:46:52.

Q. Who sent it?

A. Josh.

Q. What did he say?

A. "When's gym."

Q. Was that unusual for the defendant to ask you to go to the gym?

A. No.

Q. How often did you go to the gym together?

A. Four days a week.

Q. How did you respond?

A. I responded later with a -- oh, I said, "When do you want to go."

Q. You mentioned later. What time did you send your response?

A. 17:47.

Q. Did he respond to your question at that time?

A. No.

MR. KAMARAJU: Ms. Hurst, can we pull up just for the witness and the parties and the Court Government Exhibit 1255.

Q. I think it's on your screen now, sir.

A. I can see it.

Q. It is a little difficult, so let's blow up the left side of the screen. Do you recognize what we're looking at?

A. Yes.

Q. How do you recognize it?

A. It is a screenshot I took.

Q. What is it a screenshot of?

A. It a screenshot of, in the bottom you can see a VM being reverted and then a snapshot removed.

Q. It is a screenshot of a computer screen?

A. Yes, of my computer screen.

Q. What date and time did you take this screenshot?

A. The date was April 20, and time was 6:56 p.m.

Q. What year was that?

A. 2016.

MR. KAMARAJU: Your Honor, the government would offer Government Exhibit 1255.

MS. SHROFF: We have no objection.

THE COURT: 1255 is received in evidence.

(Government's Exhibit 1255 received in evidence)

MR. KAMARAJU: If we can publish that, Ms. Hurst, and let's just focus on that part of the screen.

Q. Let's look at the bottom there. Do you see under the title "recent tasks"?

A. Yes.

Q. Maybe if we can, can we blow that section up. Just starting at the left. What's the first entry there under "name"?

A. Remove snapshot.

Q. What's next?

A. Revert snapshot.

Q. What does it list the status as?

A. Completed.

Q. And who is it initiated by?

A. Root.

Q. If we could scroll over a little bit. What's the start time listed there?

A. Of which one?

Q. The top one.

A. The top one is 6:55 p.m.

Q. Can we scroll back. What's the second entry?

A. Revert snapshot.

Q. What's listed as the target?

A. The INF Confluence.

Q. What's the status?

A. Completed.

Q. And who initiated it?

A. Root.

Q. What's the requested start time?

A. 6:51 p.m.

Q. Did the revert snapshot task happen before the remove snapshot task?

A. Yes.

Q. Why did you take this screenshot?

A. I was concerned that Josh was using his permissions to do something wrong.

Q. Did you try to figure out what was going on?

A. Yes.

Q. Did you try to look at any log files?

A. Yes.

MR. KAMARAJU: If we could zoom back out a little bit.

Q. Were you able to look at any log files?

A. No.

Q. On this screenshot, where would the log files appear?

A. Right in the middle where there is an entry at the top that says "log entry." This is where I believe the logs would be, if there were any.

Q. On the top-left corner, if we can blow up the phrase "log entry." Is that what you were referring to?

A. Yes.

Q. If you would be able to see log files, they would have appeared here?

A. I believe so.

Q. Did that seem strange to you that there were no log files there?

A. Yes. At first this was strange to me.

Q. Why did you think it was strange at first?

A. Just because, a system managing this many VMs should have lots of logs.

Q. Did you try to find out why there weren't any log files there?

A. I did some more digging, yes.

Q. What did you think as a result of your digging?

A. I remembered that this account that I was using was a regular user account, and I couldn't remember if the regular user accounts had administrative permissions to view logs.

Q. Did you talk to anyone about this screenshot when you took it?

A. No.

Q. Why not?

A. I think there were a few reasons. One being I had talked with Jeremy, I had had that conversation with Jeremy about removing Josh's accesses, and Jeremy at that point told me stay out of it. In addition, also, I didn't know for sure what this, what this screenshot was 100 percent. I wasn't 100 percent certain. So I didn't want to -- to bring something up that was just nothing and then add to the drama.

MR. KAMARAJU: Ms. Hurst, can we go back to Government Exhibit 719.

Q. You remember we were looking at this exhibit before?

A. Yes.

Q. The time of the message where you said "when do you want to go."

A. Yes.

Q. You told us it was 17:47; is that right?

A. Correct.

Q. Does that translate to 5:47?

A. Yes.

Q. You testified before that you didn't get a response. What's the next message in this exchange?

A. I messaged Josh.

Q. And what time did you message him?

A. At 18:32, 6:32.

Q. Why did you send him this message?

A. To ask if he was ready to go to the gym.

Q. Did he respond to this message on this system?

A. No.

MR. KAMARAJU: Ms. Hurst, can we publish Government Exhibit 726, please. This is in evidence.

Q. Do you recognize this?

A. Yes.

Q. Generally speaking, what is this?

A. It is a chat log between myself and Josh on our DevLAN system.

MR. KAMARAJU: Can we go to page 10 of the exhibit, please.

Q. Do you see a message sent by the user account Schuljo at 17:34:18 or 5:34:18 on April 19, 2016?

A. Yes.

Q. Who is Schuljo?

A. Josh.

Q. Do you see it says "I wait for you on Same Time"?

A. Yes.

Q. Is this system the same as Same Time?

A. No.

Q. What's difference between the two?

A. This is our chat system that's on DevLAN, which is a completely different environment where we did all of our coding.

Q. So, let me try to make that clear. You have to be logged into your DevLAN system to use this chat system?

A. Yes.

Q. Can we turn to page 11. Do you see a message sent on April 20, at 18:35:39 or 6:35 p.m.?

A. Yes.

Q. Who sent that message?

A. I did.

MR. KAMARAJU: Maybe if we can blow it up, Ms. Hurst.

Q. What did you say?

A. "Gym?"

Q. I think on Government Exhibit 719 you ask the same question; is that right?

A. Yes.

Q. Why did you send this message?

A. Because, like I said before, we do all of our work on the DevLAN system. So it's more likely you can get in contact with somebody on the DevLAN system because everyone at their desk can take it differently, but usually your classified system was somewhat out of view.

Q. Did he respond to this message?

A. Yes.

Q. When did he respond to this message?

A. 18:37, 6:37.

Q. So, about how long after your first message?

A. A minute-ish.

Q. What did he say?

A. He said, "Yo. 15?"

Q. And what did you understand him to mean by that?

A. Do you want to go to the gym in 15 minutes.

Q. Did he explain why he didn't respond to your Same Time message?

A. He did.

Q. Did you end up going to the gym with the defendant that night?

A. Yes.

Q. Did you talk to him about what you had seen on DevLAN?

A. No.

Q. Why not?

A. Because I was not 100 percent sure, so I didn't want to say something and then Josh get upset that I was accusing him of something wrong, and that create a whole bunch of drama.

Q. Did the defendant ever stop working at the CIA?

A. Yes.

Q. When did that happen?

A. Months after moving to RDB.

Q. Did you talk to him after he left?

A. Yes.

Q. Did you ever visit him in New York?

A. Yes.

Q. After the defendant left the CIA, did you learn of -- did there come a time when you learned that EDG projects had been compromised publicly?

A. Yes.

Q. When was that?

A. On the date of the leak.

Q. How did you find that out?

A. I was just at work and a news article came out, and then it just got spread about really quickly.

Q. What was your reaction when you heard about it?

A. Kind of shock. You just, like, can't believe this is real. How -- concerned how much got leaked, how did this happen.

Q. Did you ever talk to the defendant about it?

A. Yes.

Q. Can you tell us what happened.

A. That night, when I got off work, I either had some text messages or he sent me some text messages shortly after I got off work, and he asked me, hey, man, you know, can't believe that, what are you hearing about these leaks.

Q. Other than text messages, did you ever speak with him?

A. Yes. I didn't reply to the text messages. And so then he called me.

Q. What did you talk about?

A. There was some light pleasantries in the beginning, how's New York, whatever. Then it was back to what are you hearing about this leak. You know, I'm hearing some thing I don't like.

Q. What did you understand him to mean?

A. That he had heard something about these leaks, and from someone, and he didn't like what he had heard about it.

MR. KAMARAJU: Ms. Hurst, can we publish Government Exhibit 809, please. Can we go to page 10 of the exhibit. If we can blow up the top part.

Q. Sir, do you see where this document says, "Additionally, tool described in vendor report is in fact Bartender, a CIA tool set for operators to configure for deployment"?

A. Yes.

Q. Is it true that Bartender is a CIA tool?

A. Yes.

Q. How do you know that?

A. I worked on it.

Q. How long did you work on it for?

A. Many years. I was brought on in 2013. Jeremy described -- or said that he advocated for me to join the team because he wanted me to work on this project.

Q. Prior to your testimony today, have you ever confirmed publicly that Bartender is a CIA cyber tool?

A. No.

Q. Why not?

A. Confirming any CIA tool brings danger to our operators, and it makes it difficult for us to collect foreign intelligence. When I first saw this, I just can't believe whoever wrote this would write that. It's not something we do. Putting these types of things down in paper, especially if this letter was not a classified document.

MR. KAMARAJU: I have no further questions at this time, your Honor.

MS. SHROFF: May I, your Honor?

THE COURT: Yes, you may.

CROSS-EXAMINATION

BY MS. SHROFF:

Q. Good afternoon, sir.

A. Hello.

Q. So you testified when you took the stand that you are on administrative leave. Correct?

A. Yes.

Q. And you were put on administrative leave from the CIA; is that right?

A. Yes.

Q. And how many years had you been working there when they put you on administrative leave?

A. Nine.

Q. You had been an employee for them for nine years?

A. Yes.

Q. And is it your testimony today, sir, that after nine years of working at the CIA, the CIA put you on administrative leave, and did not tell you why?

A. Yes.

Q. They didn't give you a reason?

A. No.

Q. They didn't tell you orally why they were putting you on administrative leave?

A. No.

Q. They didn't tell you in writing why they were putting you on administrative leave?

A. No.

Q. They just gave you no explanation as to why you were being put on administrative leave?

A. Correct.

Q. Did they just come up to you one day and say, You're out, you're on administrative leave, bye?

A. No. They called -- my division chief called me, and said Monday we'd like to meet you at a different entrance than you normally come in. And then on Monday when I went there, my division chief was there followed by two other people. And they told me your status has changed to paid administrative leave.

Q. And how long did this meeting last?

A. An hour, maybe two.

Q. So, for two hours, they sat down and talked to you, and in those two hours, you walked out of that meeting still not knowing why you were put on administrative leave?

A. They did not tell me.

Q. Did you ask?

A. Yes.

Q. Was there any formal procedure at the CIA by which you could ask in writing or orally as to why you were being treated that way?

A. I am not aware.

Q. Did you hire a lawyer to ask?

A. No.

Q. It is your testimony, am I correct, that at no time did the CIA tell you that it was because of your conduct during this investigation that they put you on administrative leave?

A. Correct.

Q. You did not know that?

A. They did not tell me that.

Q. Now, how many people were at this meeting that you attended, sir?

A. Probably four or five.

Q. And you said your division chief was there?

A. Yes.

Q. Which division were you in at that time?

A. I was in the cyber operations group. A division inside of that.

Q. And could you just tell me who was your division chief? You can just give me his first name if you want.

A. That's -- we're good with that?

MR. KAMARAJU: Your Honor, can I have one quick moment with Ms. Shroff.

THE COURT: Yes.

(Counsel conferring)

MS. SHROFF: Your Honor, may we just have a quick sidebar?

THE COURT: Yes.

(Continued on next page)

(At sidebar)

MS. SHROFF: Mr. Kamaraju doesn't know if the person is covert or overt, so I can just move on from that. It's OK.

THE COURT: Mr. Kamaraju.

MR. KAMARAJU: I believe that's the witness's concern.

MS. SHROFF: It's OK. I can handle that.

THE COURT: All right.

MS. SHROFF: I do have another issue, your Honor.

Late last night, Mr. Kamaraju was kind enough to send us a letter, telling us that this gentleman had been put on administrative leave and that they were paying his airfare. I reached out immediately to the CISO, because we had subpoenaed this witness and we had asked to speak to him. And during the time that we asked to speak to him, apparently he was not with the CIA anymore; he was on administrative leave. We contacted the walled attorney, and nobody told us that he was on administrative leave.

THE COURT: It's news to me.

MS. SHROFF: I know, but I think that's inappropriate. I think we're entitled to find out from the walled CIA person why they were not called, why it was not made clear to us. I attribute no bad faith to Mr. Kamaraju, but to tell us the night before, especially when I hadn't known ahead of time, it's prejudicial to Mr. Schulte.

THE COURT: Let's take this up -- you have a half an hour. Can you fill up a half an hour?

MS. SHROFF: OK. I'll fill it up.

THE COURT: We can take this up at 3:00.

MS. SHROFF: Thank you.

(Continued on next page)

(In open court)

THE COURT: Ms. Shroff.

MS. SHROFF: Sorry about that.

Q. You said that the meeting lasted about two hours?

A. Yeah. I don't know the exact amount of time, but somewhere between an hour and two hours.

Q. And at the end of that meeting, did they just simply escort you out after nine years of service?

A. Yes.

Q. OK.

A. Well, no. They asked for my badge, some other items that I did not have on me, so I had to go home, grab those items and then bring it back.

Q. OK. And you're working now, though, right? Are you working somewhere else now?

A. No.

Q. OK. But is the CIA paying you?

A. Yes.

Q. OK. Let me just take you back, setting aside this administrative-leave issue, we may come back to it later on, but for now I'd like you to just focus on the first time that you spoke to the FBI. OK?

A. OK.

Q. And is it fair to say, sir, that the FBI contacted you while you were an employee of the CIA?

A. Yes.

Q. And they asked to speak with you, correct?

A. Yes.

Q. And when they asked to speak with you, did they inform you that talking to them was voluntary, or did they not tell you that?

A. They told me.

Q. They told you it was voluntary, right?

A. Yes.

Q. And they told you your obligation was to tell them the truth, correct?

A. Yes.

Q. And they also told you not to tell anyone that you were talking to them, correct?

A. Yes.

Q. And in fact, they went a step beyond that; they told you that they so didn't want you to tell anyone about you talking to them that they made you sign what is called a nondisclosure agreement, correct?

A. Yes.

Q. It's a typed-up form, correct?

A. Yes.

Q. And it tells you that you are voluntarily talking to the FBI, right, but that you should tell no one?

A. Yeah. I don't remember what the form said, but yes.

Q. And even though you don't remember what the form said, you generally agree that you were not allowed to tell anyone that the FBI was asking you questions, correct?

A. Yes.

Q. And you signed that form, right?

A. Yes. I believe it was we could not discuss the contents of the meeting.

Q. It was just so that you didn't discuss the contents of the meeting or that you'd met with the FBI; which one?

A. I believe it was just the contents of the meeting.

Q. Did you sign that form?

A. Yes.

Q. And when you signed that form, who was in the room with you; do you remember?

A. An FBI agent.

Q. Who?

A. I don't remember which one.

Q. OK. Was there more than one FBI agent; do you remember?

A. I think so.

Q. Did they set up that meeting with you, or no?

A. Did the FBI set up the meeting?

Q. Right.

A. No.

Q. They just sprung it on you and said, Hey, come on down?

A. Yes.

Q. OK. And you were not anticipating meeting with the FBI on that particular day, right?

A. I believe so.

Q. OK. And did you think you had a choice in talking to the FBI when you went down?

A. Uh --

Q. I'll withdraw that. Let me ask you a preliminary question.

Were you surprised that the FBI was there asking to speak to you?

A. No.

Q. Huh?

A. No.

Q. You were not surprised?

A. No.

Q. And at that time, when the FBI first approached you, you were not on administrative leave, correct?

A. Correct.

Q. You were a full-time CIA employee, correct?

A. Correct.

Q. And you were not surprised, but you were not expecting the meeting, right?

A. Correct.

Q. So you went downstairs and you met with the FBI?

A. Correct.

Q. OK.

A. Went upstairs.

Q. Say it again.

A. Upstairs.

Q. Upstairs. OK. I don't know. I've never been there, but sorry about that.

This was in March of 2017, right?

A. I do not remember the date.

Q. It's OK. And you're right. Let me show you what is 3550-02. OK?

Is this the nondisclosure agreement that you signed?

A. This is my signature.

Q. It is, right?

A. Yes.

Q. OK. May I just have it back.

Thank you.

Now, was it your understanding of signing this agreement that you could tell people that the FBI had contacted you at the CIA but that you couldn't talk about the contents of what they asked you?

A. Yes.

Q. OK. So you were free to tell people that the FBI was interviewing you at the CIA?

A. Yes.

Q. Are you sure?

A. I wouldn't, but yes.

Q. You wouldn't tell anybody that the FBI had come to interview you?

A. Yeah. I wouldn't have a reason to tell anybody that.

Q. OK. And did you read this before you signed it?

A. Uh, yes.

Q. Did you agree with what it said, or did you just sign it because it was easier to sign?

A. I agreed with the principle of not discussing the contents of the meeting.

Q. OK. And after you signed this document, you sat down and were interviewed by the FBI, right?

A. Yes.

Q. And when they started to talk to you about the -- when they started the interview, did they tell you that there was a distinction between the FBI asking you questions and anything that the CIA did to you as a result of the interview?

A. Sorry. Can you restate the question?

Q. Sure.

THE COURT: It's a little bit confusing.

MS. SHROFF: It is confusing.

Q. The FBI was there in an investigatory, criminal capacity, correct?

A. Correct.

Q. And the FBI had literally the ability to arrest not just you but anyone, correct?

A. Yes, with --

Q. Right.

A. -- some --

Q. And you know that, right?

A. Right.

Q. From even just watching a movie, you know that the FBI can arrest people, correct?

A. Yes.

Q. And there's a distinction, then, between that kind of questioning and questioning that could come from within the CIA, correct?

A. Correct.

Q. I mean, your boss could interview you, question you and not like the answers, but he couldn't arrest you, correct?

A. Correct.

Q. So they're two separate inquiries, correct?

A. Correct.

Q. And when the FBI started to talk to you, did they make a distinction between the two separate inquiries for you?

A. I don't remember such a distinction.

Q. OK. Let me show you a document, and maybe that will help you remember. Is that OK?

A. Yeah.

THE COURT: Do you have a question?

BY MS. SHROFF:

Q. If you're ready, I can ask the question.

A. Sorry. I'm just reading all the bullet points.

OK.

Q. OK. Does this refresh your recollection that at least at some point you learned that there was a distinction between the FBI questioning you and the CIA questioning you? Correct?

A. Yes.

Q. OK.

A. This was not the first meeting, though.

Q. I understand.

A. OK.

Q. So somewhere down the line, when you met with the FBI again is when they explained to you that there is a distinction between a CIA questioning and an FBI questioning, right?

A. Yes.

Q. Let's just stay with the first time that you met with them, right, the FBI.

A. OK.

Q. And when you first met with the FBI, they asked you questions about your relationship with Mr. Schulte, correct?

A. Yes.

Q. They asked you a whole series of questions, correct?

A. Yes.

Q. And you did your very best to answer them, correct?

A. Yes.

Q. And how long did that interview last; do you remember?

A. I do not remember. A long time.

Q. It was a long interview, correct?

A. Yes.

Q. They asked you a series of questions, almost all of which were about Mr. Schulte, correct?

A. Yes.

Q. They asked you how you knew him, correct?

A. I don't remember their questions.

Q. You don't remember the questions at all?

A. No.

Q. OK. Do you remember they asked you about Josh Schulte?

A. Yes.

Q. OK. And did they ask you how you had known him?

A. I don't remember the specific questions.

Q. Did they ask you about your relationship with him prior to you and him working at the CIA?

A. Prior to us working? I don't remember that question. Before we came, before both of us started at the CIA?

Q. Right.

A. If we had known each other?

Q. Right. Did the FBI --

A. Sorry.

Q. I don't want to talk over you. You go.

A. Are you asking if they asked me if I had a relationship with Josh before we worked together at the CIA?

Q. Right.

A. I don't remember that question.

Q. And do you remember if they asked you about your work at the CIA and how you came to them as an intern? Do you remember that?

A. No. The very first meeting is much of a blur.

Q. All right. Let me give you 3550-01. OK?

A. Do you want me to read this whole thing?

Q. Well, just take a look at the second paragraph, and I think the word "intern" might just pop out at you, if we're lucky.

A. I don't see the word "intern --"

Q. OK.

A. -- in the second paragraph.

Q. It's all right. You know what? I'll move forward.

Do you recall the FBI asking you just general questions about where you were working, and which -- where Mr. Schulte was working while you two were friends at the CIA?

A. Yeah.

Q. And you gave them background information on yourself, correct?

A. Yes.

Q. And you gave them background information on Mr. Schulte, correct?

A. Yes.

Q. And you were asked what your opinion was as to how the information was leaked to WikiLeaks, correct?

A. I don't remember the specific question.

Q. OK. Well, why don't you take a look at the end of that document.

A. The last paragraph?

Q. Yes, please.

MR. KAMARAJU: Your Honor, I would to object to Ms. Shroff eliciting an opinion of the witness.

THE COURT: Overruled.

A. I've read the last paragraph.

Q. They asked you, and you just basically told them what your opinion was, right; it wasn't complicated?

A. Uh, the last paragraph states that I had nothing to do with the release. Is that what --

Q. No. I'm talking about the first page. Are you still on page 1?

A. The first page?

Q. Yes. 3550-01.

A. 3550-01.

Right here?

Q. Yes.

A. OK. I've read the paragraph.

Q. OK. So they asked you an open-ended question, and you tried your best to answer them, correct?

A. Yes.

Q. And when you met with them, you had no idea, correct, how this got to WikiLeaks?

A. Correct.

Q. And in fact, it is your position today that you really don't know how the information got to WikiLeaks, correct?

A. Correct.

Q. And you told them it could be a technical penetration by a foreign entity, correct?

A. Correct.

Q. And you told them it could be an inside job, correct?

A. Correct.

Q. It could be any person within the CIA, correct?

A. I didn't say that.

Q. How about by -- saying by a person or people?

A. Yes, I said that it was not -- I don't think I meant anyone. I probably meant more someone closer to that data.

Q. OK. So you thought it could be a person or people. People is plural, correct?

A. Correct.

Q. So it could be one person or it could be many people, correct?

A. Correct.

Q. And then you said, did you not, to the FBI that you thought it could be a human exploit, correct?

A. Correct.

Q. And that you thought, and then they asked you about the information itself that was leaked, right?

A. I -- it does say that here.

Q. Right. I understand, it's been a long time; you may not remember.

A. Right.

Q. And then they asked you many, many questions, did they not, about the physical security at the CIA, and then they also asked you about the security on DevLAN, correct?

A. I don't remember questions about security on DevLAN. I don't remember questions about physical security.

Q. OK. Well, do you recall telling the FBI during that meeting that anyone could check out a hard drive, bring backpacks or bags in and out of the CIA building without being searched?

A. That is true. I don't know if I said that. It does say that here in this document, in the next page.

Q. OK. But it is true, correct?

A. It is true, yes.

Q. So even though there are all these armed guards standing out with big guns, nobody really checks anybody coming in or going out, correct?

A. Provided you have the proper identification.

Q. Right. And the proper identification's just an ID, right?

A. Yes.

Q. OK. And how many people do you think have egress to that building; do you know?

A. No.

Q. Hundreds?

A. Yes.

Q. Thousands?

A. I'm really guessing here. Yes?

Q. OK. Now, you told them, did you not, that when you thought of the system itself, the DevLAN system -- right -- that you thought that the DevLAN system was the wild, Wild West, correct?

A. I don't remember specifically saying that, but I do have an opinion like that, yes.

Q. OK. And it wasn't just your opinion, right? I mean, a lot of people use the same phrase when describing DevLAN, correct?

A. Yes, all these coworkers, if we talked about the security of DevLAN.

Q. And everybody called it the wild, Wild West, correct?

A. I don't know, but, yes, they would --

Q. Well, you know what, you're not even there, so how do you know everybody said?

A. Right.

Q. When people talked about DevLAN, that's the phrase they used, correct?

A. I don't know if they called it the wild, wild -- but yes, the sentiment about it being the wild, Wild West, yes, people, everyone, coworkers have that sentiment.

Q. And the reason coworkers have that sentiment is because the system wasn't locked down, correct?

A. Correct.

Q. And it's fair to say, is it not, that the system not being locked down was partially a deliberate decision by the management at the CIA? Correct?

A. I don't know.

Q. You don't know?

A. No.

Q. OK. Is it fair to say that there was some discussion or some conversation about how people would want an open system so that they could develop tools?

A. Yes.

Q. Right?

And then that some people thought the system was too open and left you at risk, correct?

A. Yes.

Q. I don't mean you personally. I mean the CIA. Correct?

A. Yeah. In talks with other coworkers, people, we would always weigh those, the benefits versus the cons of that.

Q. Right. And management knew about these discussions, correct?

A. I don't know.

Q. Well --

A. Are we -- what level of management are we talking about?

Q. Just your boss, your immediate boss.

A. My immediate manager, yes.

Q. And at that time, in 2016, who was your immediate boss? Just give me a first name, or whatever name that --

A. Sean.

Q. Sean. And is it fair to say that there was, like, an easy kind of -- it was an easy relationship with your boss, correct?

A. Yes.

Q. I mean, you could tell him I think that the system is too wide open, correct? It wasn't like you were scared to tell him something like that, right?

A. Yes, it was easy to talk to Sean.

Q. Right. And it certainly wasn't something that Mr. Schulte would be shy about sharing, correct?

A. Correct.

Q. And in fact, he wasn't shy about sharing anything; is that fair to say?

A. Yes.

Q. And these are people that felt the system was not locked down, correct?

A. Correct.

Q. In fact, as his close friend, or at least as a friend, he complained to you nonstop about many things at the CIA, correct?

A. Nonstop is a bit strong, but yes, we did have discussions about things that irked us at the CIA.

Q. Right. I mean, he told you about things that irritated him about the CIA, correct?

A. Yes.

Q. And you told him things that irritated you about the CIA, right?

A. Yes.

Q. It's a normal job thing, correct?

A. Yeah.

Q. And one of the things that he pointed out that he thought was so silly or irritating is that it took forever to fill a requisition form, correct?

A. Yes.

Q. And he also complained about the fact that he couldn't get the system working as fast as he wanted it to work, correct?

A. Yes.

Q. And then he also complained to you about how he did not think that the system was secure enough, correct?

A. We -- are we talking about the specific system, or are we just talking about in general?

Q. I'm talking about DevLAN.

A. DevLAN? Yes.

Q. OK. And you had basically what is called a DevLAN box, correct?

A. Yes.

Q. And he also had a DevLAN box, correct?

A. Yes.

Q. Everybody had a DevLAN box that worked in your group at that time, correct?

A. No.

Q. No?

A. No.

Q. Oh, I'm sorry. Can you help me out? Most developers had a box?

A. Yes.

Q. Did all developers have a box?

A. Yes.

Q. And by box, you just mean -- that means something that hooked you on to DevLAN, conversation?

A. Yes.

Q. And do you remember there being a conversation about how developers were given free rein to use thumb drives at work?

A. A conversation about it?

Q. Yes.

A. I don't remember a specific conversation.

Q. But it's true, right?

A. We were -- we were supposed to go out and go to another team, ISB, and check out our thumb drives.

Q. Yes, but that's what you were supposed to do?

A. Yes.

Q. Nobody did that, right?

A. Most people did that.

Q. Most people did that; they checked out a thumb drive?

A. Yes.

Q. And what did they do after they used it?

A. You'd keep it.

Q. Did they check it back in?

A. No.

Q. OK.

A. Once you checked it out, it was yours to keep until you no longer wanted it one.

Q. OK. And if you lost that thumb drive, did you go get another one?

A. Yes.

Q. If you misplaced it, you could go get another one?

A. Yes.

Q. There was no limit on how many thumb drives you could get?

A. Not that I was aware of.

Q. OK. And is it fair to say that you told the FBI, when they asked you specifically about thumb drives, that thumb drives were in and out all the time? Do you remember that?

A. I don't specifically remember saying that. Could you point me to where you're at?

Q. Take a look at page 3, maybe.

A. I'm still not seeing it.

Q. OK.

A. Sorry.

Q. Well, you do agree with me, though, that people could -- thumb drives were in and out of systems all the time?

A. Yes. We -- we used thumb drives on a daily basis.

Q. OK. And I'm correct, am I not, that the only training that anybody at the CIA, or specifically within your group, received on working or using thumb drives was a one-time training when you started work there, correct?

A. When I first started --

Q. Yes.

A. Yes.

Q. Right. And is it fair to say that it was also just a one-time training that when a person, you included, started work at the CIA, you got a class on how to classify something? Correct?

A. Yes.

Q. And they told you this is how you do it, they gave you a guide and then they send you on your way, correct?

A. Yes.

Q. And that's how you decided you would mark something classified or unclassified in an email, correct?

A. Yes.

Q. OK. Now, when you were meeting with the FBI, they asked you about Mr. Schulte, and you told them, did you not, that Mr. Schulte was reliable? Correct?

A. Yes.

Q. You told them he was hardworking, correct?

A. Yes.

Q. And you told them that he had good security practices, correct?

A. I don't remember specifically saying that, but --

Q. All right. Well, take a look at page 3. It's the first paragraph.

A. OK. Yes.

Q. And in that paragraph, right, you say that he had good security practices? Right?

A. Yes.

Q. OK. Now, let me just ask you something. When the FBI came to talk to you, did they ask you about anybody other than Mr. Schulte?

A. I don't remember.

Q. OK. And you told them that despite all of these positive things, Mr. Schulte had filed several complaints to management about a person named Amol, correct?

A. Yes.

Q. And that Amol and Mr. Schulte did not get along, correct?

A. Correct.

Q. And then there were several FBI interviews asking you just about Mr. Amol and Mr. Schulte, correct?

A. Uh, I don't remember a whole interview dedicated to just Josh and Amol.

Q. OK. Do you remember them asking you about it?

A. In general, I remember, after I brought it up, they wanted to know more about the situation.

Q. OK. Before I forget, let me just ask you something, because I'd forgotten this question when I was talking to you about thumb drives. OK? Did you reuse thumb drives?

A. Like after you, like, reuse when you plug it out and then the next day, just plug it back in?

Q. Right. Or if you finished project 1 and you're moving on to project 2, did you reuse the thumb drive, or did you just --

A. We reused it.

Q. And before you would reuse it, would you reformat the thumb drive?

A. Not all the time.

Q. Sometimes?

A. Sometimes.

Q. Would you clean out the project you were working on before you get started?

A. Clean out the thumb drive is what you're saying?

Q. Right.

A. No, that wasn't standard procedure.

Q. So what did you do if the thumb drive had one project on it and you wanted to start a second project on it?

A. If I was done with the first project --

Q. Right.

A. -- depending on what that project did --

Q. Right.

A. -- I would either wipe it securely or just delete the files logically.

Q. Right.

A. Or --

Q. Let's talk about that. What does it mean when you say wipe it?

A. Wipe it securely?

Q. Right.

A. That means to overwrite the data on the drive with new data such that, so that now that old data can no longer be read.

Q. OK. So you get rid of the old data, correct?

A. Correct.

Q. And what was the second thing you said?

A. Or if -- if I didn't care that the drive needed to be secure, I would just logically delete the files.

Q. OK. And is that called zeroing a thumb drive?

A. No. That was the first thing.

Q. The first thing is called zeroing a thumb drive, and then the second thing is called just wiping?

A. Just deleting. Wipe means -- wipe implies a secure delete. The second thing is just a normal, just how you would plug it in and delete files.

THE COURT: Ms. Shroff, is this a convenient place to break?

MS. SHROFF: Sure.

THE COURT: Remember my instructions.

Please be seated. Please be seated.

Remember my instructions. Don't talk about the case. Don't do any research. If you hear anything about it on the radio or the TV, ignore it.

Keep an open mind, and I'll see you tomorrow morning at 9:00.

(Continued on next page)

(Jury not present)

THE COURT: Please be seated.

MS. SHROFF: Your Honor, may we excuse the witness?

THE COURT: Oh, yes.

You're excused.

THE WITNESS: Leave all these documents here?

THE COURT: Yes, leave all of it. Don't talk to the government now. You're on cross-examination.

(Witness not present)

THE COURT: OK. Ms. Shroff, do you want to take up what --

MS. SHROFF: Your Honor, I --

THE COURT: OK. He's out of the courtroom.

MS. SHROFF: I don't mean to belabor this point, and I, again, want to be clear I was informed last evening that this gentleman, this witness, had been put on administrative leave at some point by the CIA. I think it was June of -- August of 2019. Right?

And the only, first reason I was given was that somebody at the CIA told Mr. Kamaraju that that was because of his conduct during the investigation.

One, I do not know why we were not told, because we had subpoenaed this gentleman and asked if he would speak to us, that he was in fact put on administrative leave. I asked the CISO, and I don't have an answer on that point.

Second, even if the CIA doesn't want to tell him why they put him on administrative leave, I do think we are entitled to know why because of the flag, so to speak, that they've set out by saying that it was his conduct during this investigation.

Now, unlike many of the 302s that I've read in this case, where everybody said, Oh, it had to be Mr. Schulte, this gentleman actually at one point, early on in the process, said that it wasn't Mr. Schulte; he didn't think it was Mr. Schulte; that Mr. Schulte was hotheaded but not a traitor, and then slowly, slowly, slowly, his story started to morph a little, but he never quite got to saying it was Mr. Schulte.

Now, I don't know -- I honestly don't know -- what the thinking of the CIA is, but I do think it's fair for us to know what their thinking was as to why they put him on administrative leave. I'd ask the Court, please, to order the CIA or the government to produce to us those files, or at least produce them to you for *in camera* reading so that you can determine whether or not we should be entitled to them.

THE COURT: Mr. Kamaraju.

MR. KAMARAJU: Yes, your Honor.

THE COURT: When was he placed on administrative leave?

MR. KAMARAJU: August 19, 2019.

THE COURT: OK.

MR. KAMARAJU: Which was three days after the meeting that Ms. Shroff discussed.

I think one point we should make clear, he is still a CIA employee. The fact that he's an administrative leave does not change that fact. There are situations where people on administrative leave come off administrative leave. He's being paid by the CIA, so he's a CIA employee. Yes, currently he's on leave.

The reasons for that leave -- actually, we produced all of the underlying information to Ms. Shroff. It is these 302s. It's videos of security. It's the interview notes. And as I said to Ms. Shroff, as reflected in the 302s, there was a concern about candor. The materials underlying that concern about candor have been produced.

Everything Ms. Shroff just said that she'd like to do on cross-examination she can do. She's already spent a portion of her time on cross-examination eliciting the fact that he said positive things about Mr. Schulte during the first interview. I don't quite agree with her characterization that he exonerated Mr. Schulte in any way, but still, to the extent she wants to elicit the time line of events, she's able to do that. To the extent she wants to try and make the argument that he was telling a positive story about Mr. Schulte until events went a certain way and the CIA took action, she's able to do that.

THE COURT: Why was he put on administrative leave?

MR. KAMARAJU: It's because exactly that, your Honor. It's because, as I understand it, there were concerns about his candor, which we disclosed in the letter that we sent. The actions were the result --

THE COURT: What letter did you send?

MR. KAMARAJU: I'm sorry, your Honor?

THE COURT: What letter did you send? I don't recall getting a letter.

MR. KAMARAJU: No, no, your Honor. It's the letter informing Ms. Shroff.

THE COURT: Oh, Ms. Shroff. OK.

MS. SHROFF: I got it last night, your Honor.

MR. KAMARAJU: Yes, but all of the materials that underlie those concerns -- for example, there's a video of an interview he did with the CIA investigator about the fight that he testified about; he refused to talk about that fight. That's an example of something that generated the security video. And she has those materials. We produced everything in our files with respect to anybody that had access to the DevLAN system, any kind of security concerns that related to mishandling of classified information with respect to that system. He doesn't have any of those.

THE COURT: From your standpoint, Mr. Kamaraju, Ms. Shroff can go into all this on her cross-examination?

MR. KAMARAJU: She's certainly entitled to question his credibility on cross-examination, and she's certainly entitled to question whether he has a bias or feels pressured to tell a story, so to speak, which is what I understand her to want to say. But I don't think she's entitled to the internal decision-making of the CIA.

MS. SHROFF: I'm not looking for the internal decision-making of the CIA. I'm just trying to tell this jury that if you don't roll the way the CIA wants you to roll, they're going to throw you out, and of course, that's relevant. And I don't think anybody who has had a job would consider being on administrative leave --

THE COURT: As I understand it, Ms. Shroff, the government doesn't object to you going into the cross-examination.

MS. SHROFF: No, I don't want to question about it on cross-examination. I want to be able to show the jury not that he lacked candor; I want to show the jury that because of what he said, that the CIA didn't like it and the CIA retaliated against him. That's my point, which is what they did.

MR. KAMARAJU: Well --

MS. SHROFF: They --

MR. KAMARAJU: I'm sorry. I apologize.

MS. SHROFF: I don't know. I could be right. I could be wrong. But the only way I'm going to know is if either you let me read it or you read it. And since they never let me read anything hardly in this case, I'll rely on you reading it. I don't mind, but somebody's got to read it because the issue here is the way the CIA reacts when they don't like something somebody else does and that person is working for them. It's a different point, right? It isn't about whether or not he had candor. This is about what the CIA does to a person who is telling a story that they don't like.

MR. KAMARAJU: Everything that Ms. Shroff said she wants to be able to do she can do standing here right now. She can cross-examine the witness about: You said to the FBI on this day X; you said to the FBI on this day X. Then on this day, you said something different, isn't that right? And then on this day the CIA put you on administrative leave.

THE COURT: Except what Ms. Shroff is saying is what if there are documents where the CIA said: Hey, we've had enough of this guy; let's fire his ass out of here.

MR. KAMARAJU: Sure. I understand, your Honor, and we double-check, but I do not believe there are any documents that say that. The documents do not say, It's time to get this guy; he's telling the wrong story. And we're happy to give them to your Honor.

MS. SHROFF: Well, of course it's not going to say that. They're not that silly.

MR. KAMARAJU: Well, then I don't know what Ms.

Shroff's going to get from the documents.

MS. SHROFF: I don't know what it is. All I'm saying is if he can read it, why can't I? I don't understand this. And if I can't read it, I'd just ask you to read it.

THE COURT: I'll read it.

MS. SHROFF: Thank you.

MR. KAMARAJU: OK.

THE COURT: Submit it for *in camera* review.

MR. KAMARAJU: We will, your Honor.

THE COURT: Now, with regard to the experts and giving an instruction, I've decided not to do that. I think the appropriate time for the instruction is when we hear instructions.

If you want a caution about the experts and how to assess the testimony, you should have made a request to put it in the preliminary instruction to give to the jury, but I think any instructions now would put the thumb on the scale of justice, so I'm not going to do it. I will charge on experts in the final charge to the jury.

MR. KAMARAJU: We understand, your Honor. That's fine with us.

THE COURT: Anything else?

MR. KAMARAJU: No.

MR. ZAS: Just for the record, we object to that ruling. Our concern is we didn't want, sometimes juries take experts as gospel, which is really the point of the instruction. We just wanted them to know sooner rather than at the very end, which could be another several weeks. So we object to the ruling.

THE COURT: Several weeks?

MR. ZAS: Well, when the trial's over. Whenever we get there.

THE COURT: When are we getting there?

MR. ZAS: I think you're going to have to ask them, your Honor.

THE COURT: I will.

MR. ZAS: Thank you.

MR. KAMARAJU: We're going as fast as possible, your Honor, but we do not anticipate it being several weeks. Obviously, Mr. Leedom's testimony, he was a significant witness. We've got a couple more, but I don't think anybody who approaches his length, so I think we're hoping that -- we'll have a better idea by the start of next week, but I think we're hoping to be able to rest soon.

THE COURT: Let's talk about the start of next week. Are we working on Monday?

MS. SHROFF: No. It's a holiday, your Honor.

THE COURT: We can work on holidays, Ms. Shroff.

MS. SHROFF: Oh, no, your Honor. Look, I was so good. I only crossed him for 30 minutes.

MR. KAMARAJU: We'll be working on Monday, your Honor, so we don't have an objection. I don't know what the jury's plans are.

THE COURT: Do we know?

We know from our conversations that there's a number of jurors who have got plans for taking a long weekend.

MS. SHROFF: Oh, thank God.

MR. KAMARAJU: I can imagine they want to get away from us.

THE COURT: Yes, they want to revert back to a legitimate vacation schedule.

OK. I'll see you tomorrow morning at 9:00.

MS. SHROFF: Thank you, your Honor.

THE COURT: When can I expect the package, Mr. Kamaraju?

MR. KAMARAJU: We'll consult, and we'll walk it over this afternoon.

THE COURT: Thank you.

(Adjourned to February 13, 2020, at 9:00 a.m.)

INDEX OF EXAMINATION

GOVERNMENT EXHIBITS